



Ivanti Policy Secure Administration Guide
9.1R14

Copyright Notice

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.lvanti.com.

Copyright © 2022, Ivanti. All rights reserved.

Protected by patents, see <https://www.ivanti.com/patents>.

Contents

Preface	11
Document conventions	11
Requesting Technical Support	12
Reporting Documentation Issues	14
Revision History	15
Introduction to Ivanti Policy Secure	19
Overview	19
IPS Components	20
IPS Enforcement Modes	21
Profiler	23
Overview	23
Roles, Realms and Sign-In Policy	25
Overview	25
User Roles	27
Authentication Realm	40
Sign-in Policies	56
Managing Sign-In Policies	62
Configuring Sign-In Notifications	65
Configuring Sign-In Pages	68
Using the Initial Setup Wizard	72
Overview	72
Configuring IPS using Initial Setup Wizard	73
Verification and Troubleshooting	98
IPS Migration Wizard	100
Layer 2 Enforcement	109
Policy Enforcement using 802.1X	110
Overview	110
Benefits of 802.1X Authentication	110
Deployments using 802.1X Authentication	111
Configuring 802.1X on IPS	115
Policy Enforcement using MAC Authentication	157
Overview	157
Benefits of MAC authentication	157
Deployments using MAC Authentication	157
Configuring MAC Authentication on IPS	159
Policy Enforcement using SNMP/SSH	175
Overview	175
Benefits of SNMP Enforcement	175
Policy Enforcement Using Simple Network Management Protocol/SSH	175
Configuring SNMP Policy Enforcement using VLAN (Cisco, HP)	179
Configuring SNMP Policy Enforcement through Templates using ACL/VLAN	191
Appendix	201

Policy Enforcement using 802.1X Native Supplicant	211
Overview	211
Benefits	211
Deployments using 802.1X Authentication with Native Supplicant	211
Configuring Agentless Host Checking with Native Supplicant	214
Configuring 802.1X for Native Supplicant on IPS	217
Configuring Native Supplicant for 802.1X Authentication	217
Layer 3 Enforcement	230
Enforcement using Check Point Next-Generation Firewall	231
Overview	231
Deployment of IPS using Check Point Next-Generation Firewall	231
Deployment of IPS with Check Point Next-Generation Firewall for a Large Enterprise	232
Configuring IPS with Check Point Next-Generation Firewall	233
Configuring Check Point Next-Generation Firewall	239
Troubleshooting	243
Unsupported Features	243
Enforcement using Palo Alto Networks Firewall	244
Overview	244
Deployment of IPS using PAN Firewall	244
Configuring IPS with PAN Firewall	248
Configuring Palo Alto Networks Firewall	256
Troubleshooting	263
Unsupported Features	265
Enforcement using FortiGate Firewall	266
Overview	266
Deployment of IPS using FortiGate Firewall	266
Configuring IPS with FortiGate Firewall	267
Configuring FortiGate Firewall	268
Reports and Logging	273
Identity Based Enforcement using FortiGate Products	274
Deployment of IPS using FortiAuthenticator and FortiGate Firewall	274
Configuring IPS with FortiAuthenticator	275
Configuring FortiAuthenticator	277
Configuring FortiGate Firewall	281
Reports and Logging	284
Enforcement using SRX Series Firewall	286
Overview	286
Deployment of IPS using SRX Firewall	286
Configuring IPS with SRX Firewall	287
Configuring SRX Firewall	291
Configuring Additional TLS Settings	294
Enforcement using EX Series Ethernet Switches	296
Configuring EX switch with IPS	296
Configuring EX switch as an Infranet Enforcer	297

Enforcement using Screen OS Firewall	300
Overview	300
Deployment of IPS using ScreenOS Firewall	300
Configuring IPS with ScreenOS Firewall	301
Configuring ScreenOS Firewall	303
Appendix	311
Captive Portal	321
Deployments with Juniper IDP	325
About IDP Technology	325
IDP Deployment Scenarios Overview	326
Understanding IPS Deployments with IDP Devices	326
Activating IDP for the ScreenOS or Junos Enforcer	329
Managing Interoperation with IDP Devices	330
Identifying and Managing Quarantined Users Manually	332
Using Role-Based Policies to Monitor User Activity	333
Provisioning ICS sessions to PAN/Check Point/FortiGate Firewall	335
Overview	335
Deployment of IPS/ICS using PAN/Check Point/ FortiGate Next Generation Firewall	335
IF-MAP Configuration	336
Visibility based Firewall Enforcement	340
Overview	340
Configuring Firewall Provisioning based on Profile Group	340
One-to-One Network Address Translation	348
Overview	348
One-to-One NAT Deployment	348
Configuring one-to-one NAT	349
IF-MAP Federation	354
Overview	354
IF-MAP Federation Use Cases	354
IF-MAP Configuration	361
Active Federated Session Details	370
Troubleshooting	372
Appendix	373
Behavioral Analytics	380
Overview	380
Licensing	382
Benefits	382
Configurations	382
Pre-Requisites	382
Summary of Configuration	382
Configuring IPS for enabling Behavioral Analytics	383
Dashboard and Reports	391
Troubleshooting	394
Appendix	395

IoT Access	398
IoT Policy Provisioning	398
Troubleshooting	419
Host Checker	422
Host Checker Overview	422
Policies	423
Host Checker Installation Options	428
Endpoint Security Assessment Plug-In (ESAP)	429
Understanding Host Checker Policy Remediation	442
Configuring Host Checker Policy	444
Store and Reuse Host Checker Policy Results	482
Admission Control Using Network Security Devices	485
ICS Admission Control Using IPS	486
Configuring ICS Admission Control	487
MDM Interoperability with IPS	489
Overview	489
Configuring IPS with MDM Servers	500
Configuring IPS with Pulse Workspace	526
Configuring IPS with Microsoft Intune	528
Configuring the Microsoft Intune MDM	530
Configuring the PWS MDM	538
Configuring the AirWatch MDM	538
Configuring the MobileIron MDM	543
Troubleshooting	545
AAA Servers	549
AAA Server Overview	549
AAA Traffic Management	551
Using the Local Authentication Server	555
Using Active Directory	568
Using Kerberos SSO	575
Understanding Multidomain User Authentication	576
Understanding Active Directory and Windows NT Group Information Support	578
Importing and Exporting an Active Directory Mode Configuration	579
Using the Anonymous Server	580
Using the Certificate Server	582
Using an LDAP Server	585
Using the LDAP Password Management Feature	593
Using the MAC Address Authentication Server	599
Using an NIS Server	611
Using a RADIUS Server	613
Using an ACE Server	631
Using the SAML Server	636
Access Control with SAML Server	644
SAML 2.0 Configuration Tasks	647

Using a SiteMinder Server	655
Troubleshooting the SiteMinder Server Configuration	671
Using an SQL Auth Server	672
Troubleshooting Oracle Error Codes	687
Using a Time-Based One-Time Password (TOTP) Authentication Server	687
Configuring HTTP Attribute Server	700
Cascading Authentication Support	701
Configuring MSSQL Server Accounting	703
Configuring SQL Accounting	704
Network Device Administration using TACACS+	710
Overview	710
Configuration	712
Monitoring Device Administration	723
Troubleshooting	724
Appendix	732
Two-Factor Authentication using Smart Cards	735
Guest Access	743
Overview	743
Deployments	744
Configuring IPS for WLC Deployment	748
Configuring IPS for SRX/EX Deployment	771
Configuring IPS for Guest Wired Authentication using Cisco Switch	772
Configuring IPS for Sponsored Guest Access	779
Guest Self Registration	786
Guest Self Registration for Sponsor Approved Guest Access	788
Guest User Administration	792
Customizing Guest Self Registration User Pages	805
Configuring Cisco 2500 WLC	812
Configuring Cisco 3850 WLC	833
Configuring Cisco WLC using CLI	848
Configuring Cisco 2620 for Guest Wired Authentication	849
Configuring Aruba WLC	851
Configuring Aruba Instant Access Point	871
Configuring Ruckus WLC	879
Ruckus SmartZone WLC Configuration	881
Ruckus ZoneDirector WLC Configuration	883
Cisco Meraki WLC Configuration	886
Example Configuration: Guest Access with Huawei WLC/Switch	890
Example Configuration: Guest Access with Juniper Mist WLC	908
Enterprise Onboarding	914
Overview	914
Deployments	915
Configuring Enterprise Onboarding	916
Troubleshooting	935

Clustering	936
Overview	936
Deployments	936
Cluster Configuration	938
Load Balancer for Active/Active Cluster	948
Serial Console Configuration	951
WAN Clustering	953
Monitoring and Troubleshooting	956
Appendix	963
Cloud Secure	967
System Management	968
Network and Host Administration	969
Network and Host Administration Overview	969
Configuring the Internal Port	970
Configuring the External Port	973
JITC Mode Option	976
Using the Management Port	983
Configuring VLAN Ports	989
Using Virtual Ports	992
Configuring the System Date and Time	994
Configuring NTP and Other Services Traffic Over Any Physical Interface	998
Configuring Network Services	999
Managing the Routes Table	1001
Managing the Hosts Table	1002
Managing the ARP Table	1003
Managing the Neighbor Discovery Table	1004
Configuring SSL Options	1005
Enabling Granular Cipher Selection for Setting the Security Options	1005
Configuring Health Check Options	1012
Configuring Miscellaneous Security Options	1013
Configuring Custom HTTP Headers	1016
Using the Serial Port	1018
Certificate Security Administration	1023
Understanding Digital Certificate Security	1023
Using Device Certificates	1024
Using Trusted Client CAs	1035
Using Client Auth Certificates	1047
Using Trusted Server CAs	1051
Understanding ECC Certificates	1054
File Management	1056
Overview	1056
Configuration	1056
FIPS Level 1 Support	1095
FIPS Level 1 Support Software FIPS	1095

FIPS Supported Platforms	1095
FIPS Level 1 Support	1096
FIPS Level 1 Support	1099
Supported Cipher Suites	1099
Dashboard and Reports	1104
Dashboard and Report Overview	1104
Enabling the Dashboard	1104
Using the Dashboard	1105
Using the User Summary Report	1113
Using the Device Summary Report	1117
Using the Single Device Report	1120
Using the Device Discovery Report	1124
Using the Authentication Report	1124
Using the Compliance Report	1128
Using the Infected Devices Report	1133
System Maintenance	1136
Overview	1136
Configuring System Platform	1136
Configuring System Maintenance Options	1138
Installing the Service Package	1141
Downloading Client Installer Files	1145
Testing Network Connectivity	1145
Logging and Monitoring	1147
Logging Overview	1147
Displaying System Logs	1148
Configuring Log Events Settings	1152
Log Filtering	1154
Displaying User Access Statistics	1157
Monitoring using SNMP	1157
Configuring an External Syslog Server	1167
Configuring Advanced Settings	1169
Enabling Client-Side Logging	1170
Displaying System Status	1170
Displaying Hardware Status	1172
Using Software RAID on PSA7000	1174
LCD Display	1175
Displaying Active Users	1177
Troubleshooting	1180
Overview	1180
Policy Tracing	1180
Debug Logs	1183
RADIUS Diagnostic Logs	1185
Samba Diagnostic Logs	1187
TCP Dump	1188

Network Troubleshooting Commands	1191
Troubleshooting TCP and UDP Port Status	1193
Testing Server Connectivity	1196
Kerberos Debugging	1197
Remote Debugging	1198
Using Log Selection	1199
Troubleshooting the Common Issues with IPS	1201
Appendix REST API Support	1205
Overview	1205
Sample GET/POST/PUT/DELETE Request and Responses	1208
Appendix Custom Expressions and System Variables Reference	1213
Using Custom Expressions in Rule Configuration	1213

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Ivanti technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
<i>italic text</i>	Identifies emphasis
	Identifies variables
	Identifies document titles
Courier Font	Identifies command output
	Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.

Convention	Description
<i>italic text</i>	Identifies a variable.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Non-printing characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.
bold text	Identifies command names, keywords, and command options.

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.



A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

Attention: An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

Caution: A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

Requesting Technical Support

Technical product support is available through the Ivanti Global Support Center. If you have a support contract, file a ticket with Ivanti Global Support Center.

- Product warranties—For product warranty information, visit <https://support.pulsesecure.net/product-service-policies/>

Self-Help Online Tools and Resources

For quick and easy problem resolution, Ivanti provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://support.pulsesecure.net>
- Search for known bugs: <https://support.pulsesecure.net>
- Find product documentation: <https://www.ivanti.com/support/product-documentation>
- Download the latest versions of software and review release notes: <https://support.pulsesecure.net>
- Open a case online in the CSC Case Management tool: <https://support.pulsesecure.net>
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://support.pulsesecure.net>

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: <https://kb.pulsesecure.net>
- Ask questions and find solutions at the Pulse Community online forum: <https://community.pulsesecure.net>

Opening a Case with Ivanti Global Support Center

You can open a case with Ivanti Global Support Center on the Web or by telephone.

- Use the Case Management tool in the Ivanti Global Support Center at <https://support.pulsesecure.net>.
- Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see <https://support.pulsesecure.net/support/support-contacts/>.

Reporting Documentation Issues

To report any errors or inaccuracies in Ivanti technical documentation, or to make suggestions for future improvement, contact Pulse Secure Technical Support (<https://support.pulsesecure.net>). Include a full description of your issue or suggestion and the document(s) to which it relates.

Revision History

The following table lists the changes to this document from the previous release.

Feature	Add/Update/Remove	Document Published Date/Document Version	Effective Release	Notes
Framed-IP Address Pool	Updated Configuring MAC Authentication on IPS with the following subsections: <ul style="list-style-type: none"> • IP Address Pools • Configuring IP Address Pool 	October 2021/1.0	9.1R13	
Delegated Admin Control	Updated Configuring MAC Authentication on IPS with the following subsection: <ul style="list-style-type: none"> • Delegated Admin Control 	October 2021/1.0	9.1R13	
IPS TLS Settings and MSSQL support	These sections are updated: <ul style="list-style-type: none"> • Configuring Additional TLS Settings • MSSQL Server support for Accounting • Cascading Authentication Server support 	August 2021/1.0	9.1R12	

Feature	Add/Update/Remove	Document Published Date/Document Version	Effective Release	Notes
IPS and Profiler Reporting enhancements	Updated the Dashboard and Reports section.	February 2021/1.0	9.1R11	
NetBIOS Rule	Added the maximum supported regex patterns in a NetBIOS rule.	December 2020/2.2	9.1R10	
Host Header	Updated the Configuring Miscellaneous Security Options section.	December 2020/2.1	9.1R10	
Firewall Provisioning using Profile Group	Added Visibility based Firewall Enforcement .	October 2020/2.0	9.1R9	
Support Single Logout	Support Single Logout with Pulse Desktop Client Using the SAML Server .	October 2020/2.0	9.1R9	
Support NTP pool of servers	Updated Configuring the System Date and Time .	July 2020/1.0	9.1R8	
Host Checker	Support Platform Matrix section is updated with Client/Clientless differences.	July 2020/1.0	9.1R8	
IPS and Nozomi Networks integration using generic HTTP Attribute Server	Configuring HTTP Attribute Server Pulse Policy Secure: <i>Nozomi Networks Integration Guide</i> is newly added.	July 2020/1.0	9.1R8	

Feature	Add/Update/Remove	Document Published Date/Document Version	Effective Release	Notes
IPS and McAfee ePO integration using generic HTTP Attribute Server	Configuring HTTP Attribute Server IPS and McAfee ePO integration using generic HTTP Attribute Server is newly added.	July 2020/1.0	9.1R8	
Assign RADIUS Return Attributes for Local and MAC Auth Users	Creating User Accounts MAC Address Authentication Server Overview Configuring RADIUS Return Attributes	July 2020/1.0	9.1R8	
UEBA package upload	UEBA Package	July 2020/1.0	9.1R8	
Layer 2 Enforcement	Secondary authentication not supported with 802.1x native supplicant.	June 2020/1.0	9.1R7	
Admission Control	Admission Control Policy action is not taken for endpoints behind Network Address Translation (NAT).	June 2020/1.0	9.1R7	
IPv6 Support for System Management	Added IPv6 Support under System Management. Updated Configuring the System Date and Time and Archiving .	March 2020/1.0	9.1R5	

Feature	Add/Update/Remove	Document Published Date/Document Version	Effective Release	Notes
MSSQL Auth Server Support	Added MSSQL support in AAA servers Configuring Authentication with MSSQL Auth Server .	March 2020/1.0	9.1R5	
Hard Disk Encryption	Host Checker policy to allow detection of hard disk encryption in-progress. Updated Configuring Hard Disk Encryption Rule .	April 2020/1.0	9.1R5	
Admission Control using McAfee ePO	Pulse Policy Secure: <i>Admission Control using McAfee ePO Integration Guide</i> is added.	April 2020/1.0	9.1R5	
SNMP ACL and VLAN-Huawei, Alcatel Lucent and Arista	Sample configuration added for Huawei ,Alcatel Lucent and Arista. Updated Appendix .	April 2020/1.0	9.1R5	
Splunk syslog Add-on and Dashboard added	<i>IPS and Splunk Integration Guide</i> is updated.	April 2020/1.0	9.1R5	

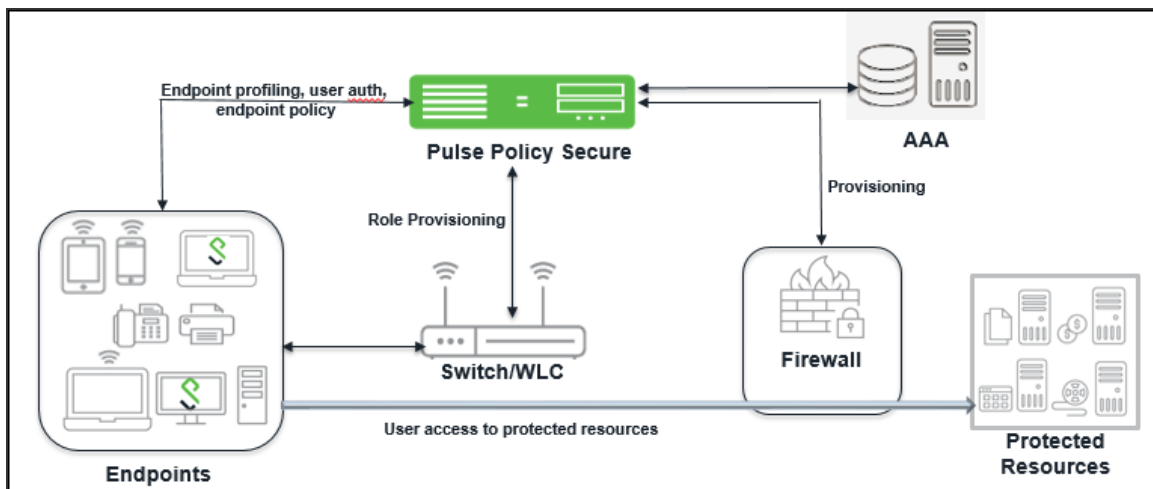
Introduction to Ivanti Policy Secure

Overview

Ivanti Policy Secure (IPS) is a network access control (NAC) solution which provides network access only to authorized and secured users and devices. It protects your network and guards mission critical applications and sensitive data through comprehensive NAC management, visibility, and monitoring.

It reduces the cost and complexity of delivering and deploying granular, identity, and role enabled access control from the branch to the corporate data center. It also addresses most NAC challenges, which includes insider threats, guest access control, and regulatory compliance.

The IPS solution leverages AAA framework, which contains the user profiles, attributes, group roles and identities. It then binds the user identity information to the endpoint and to the network and uses the resultant policy to map the user to the appropriate role during the access session.



IPS solution uses endpoint validation to place the users into specific access groups. The groups can be provisioned access to different resources based on access control mechanisms such as virtual LANs (VLAN), filters, or access control lists (ACL). You can also define additional QoS parameters for the session for role based policy enforcement so that only authorized users can access the application and data. The solution allows access only from users who are compliant with the security policies that you define. IPS also works well with unmanaged devices, such as printers, VoIP phones, and IP enabled cameras. You can configure typical hosts, such as VoIP phone, that is not 801.1X enabled to be permitted to the network using SNMP enforcement and the Profiler. The integration with Profiler enables IPS to build a database of the unmanaged devices on the network and have the same access security as managed devices. IPS solution is extremely flexible and offers numerous options for integration into your existing network. When an endpoint connects to the network, IPS gathers user authentication data, endpoint security state data, and device location. It combines the information to create dynamic policies or uses the user created policies, which are then propagated to enforcement points. The enforcement can be either at the edge of the network prior to granting an IP address using 802.1X, within the network on the firewall, or both for greater granularity.

IPS Components

IPS solution consists of the following main components:

- Ivanti Policy Secure (IPS)—A central policy management server that validates the user's identity, determines the endpoint's security compliance, and manages network policies.
- Enforcer—Policy enforcement points for user authentication. For example, switches, firewall, and WLCs.
- Pulse Client—Client running on endpoints for user authentication, device compliance using IPS.
- Profiler—It dynamically identifies and classifies endpoints across managed and unmanaged endpoint devices, so that access to network and resources can be controlled based on the type of the device.

IPS offers the following benefits:

- Centralized management of Access and Compliance policies.
- Easy integration with several Authentication, Authorization, and Accounting (AAA) servers.
- Role-based, application-level enforcement.

- Allows context-aware policy enforcement for wired and wireless connections across desktop and mobile platforms.
- Distributed enforcement of network access policies.
- Dynamic endpoint assessment and enforcement.
- Supports compliance based network access for endpoints.
- Supports comprehensive network visibility with simplified auditing, and monitoring of devices.
- Supports interoperability with existing network infrastructure such as switches, wireless controllers, AD, firewalls, IDS, and Security Information and Event Management (SIEM).
- Extends policy enforcement with information from Enterprise Mobility Management (EMM) solutions. IPS supports leading global-device management solutions from Pulse Workspace (PWS), MobileIron, AirWatch, and Microsoft Intune. IPS works with the Mobile Device Management (MDM) solution to evaluate whether the BYOD or corporate devices are compliant with organizational and MDM policies.
- Supports automated device onboarding, self-service enrollment, and integration with existing infrastructure to simplify deployments.
- Supports Simple Network Management Protocol (SNMP) in the network device definition for the Profiling service to communicate with the network devices and profile endpoints that are connected to the network devices.
- Delivers guest user access control capabilities for simple, seamless, and authorized network access to guests.
- Supports captive portal capabilities for allowing users onto their guest networks and capturing relevant information

IPS Enforcement Modes

To provision resource access policies, you can use 802.1X Layer 2 switch, access point, or firewall within any enterprise class network edge infrastructure that supports 802.1X and Remote Authentication Dial-In User Service (RADIUS).

The following types of devices can be used as IPS enforcement points:

- Infranet Enforcer (Firewall) —Devices that control traffic flow based on Layer 3 data. You can use Palo Alto, Check Point, Fortinet, Juniper Networks SRX series and Screen OS firewalls as enforcers. For more information, see Layer 3 Enforcement.
- 802.1X devices—You can use any 802.1X enabled switches or access points with IPS. The 802.1X protocol provides port based authenticated access to LAN. This standard applies to both wireless and wired networks. For more information, see Layer 2 Enforcement.

You can use 802.1X enabled switches or access points with or without the Infranet Enforcer as part of the solution. If you do not deploy the Enforcer, the 802.1X enabled switch or access point functions as the enforcement point. You can create different security zones by configuring VLANs on the network and assigning different roles to the appropriate VLAN.

Profiler

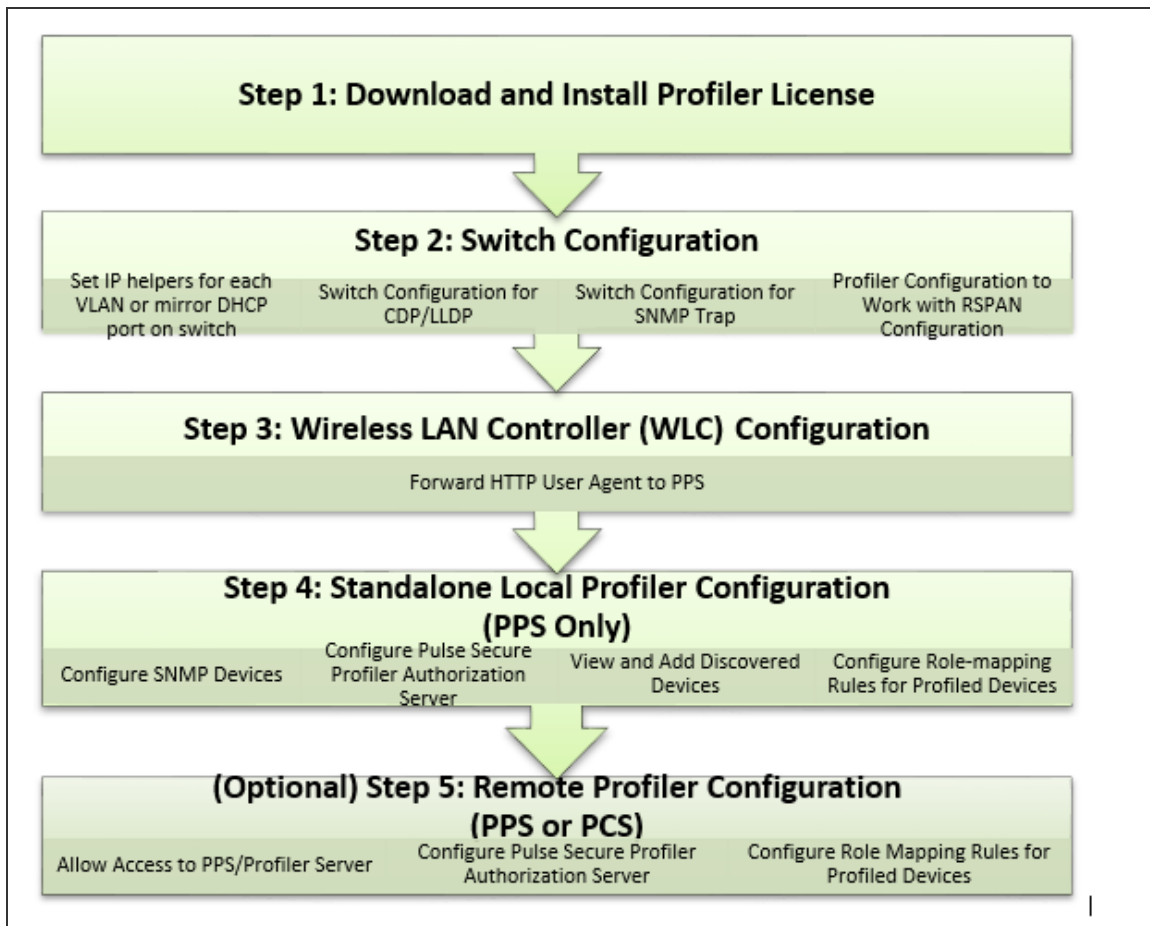
Overview

Profiler dynamically identifies and classifies endpoints across managed and unmanaged endpoint devices, so that access to network and resources can be controlled based on the type of the device. It also helps you to get visibility and enforce your security policies for corporate access, BYOD, and guest access.

The Profiler has the capability to:

- Detect and classify devices using DHCP fingerprinting.
- Provide access control for devices based on the device profile - mainly characterized by Manufacturer, Operating System, and Device Category.
- Provide visibility into IP-enabled devices connecting to the network.
- Enable MAC Authentication.
- Enable granular policies based on device attributes.

A high-level overview of the configuration steps needed to set up and run Profiler is shown in the following figure.



For more information on deployment and configuration, see *Profiler Deployment Guide*.

Roles, Realms and Sign-In Policy

Overview

IPS access management framework allows only qualified users to access protected resources. The policies are created to allow or deny access to resources based on user's role and user's endpoint device compliance. The access management framework comprises of the following key elements:

User Roles

User role is used to categorize a group of users and accordingly provide access to a set of protected resources for these group of users. User role defines the type of access and the permissions required for accessing a protected resource. Administrator can define multiple user roles for the end users.

For example:

- Employees- Users who require access to all the company resources.
- Contractors- Users who work on a contract basis and require access to selected network resources.
- Guests- Users who visit the company and require limited access to network resources.

Authentication Realm

Authentication realm specifies the conditions that users must meet to sign-in to the system. A realm contains details about the authentication server with which the user is authenticated and list of restrictions/checks that needs to be passed on the client machine.

It also includes mapping of different users to different groups or roles with the use of role mapping rules.

- Authentication Server- An authentication server is a database that stores user credentials (username, password, group, and attribute information). The user logs-in to IPS through a specific authentication realm, which is associated with an authentication server, IPS forwards the user's credentials to the authentication server to verify the user's identity through AAA framework.

The IPS supports the following authentication servers:

- Active Directory
 - RADIUS
 - LDAP
 - NIS
 - RSA ACE/Server
 - Anonymous
 - Certificate
 - SAML Server
 - SiteMinder
 - Mac Address Authentication
 - Local Authentication Server. For more information, see [Local Authentication Server Overview](#).
- Authentication Policy- It is a set of rules and restrictions to control resource access.
 - Role-Mapping- It consists of conditions a user must meet for IPS to map the user to one or more user roles. These conditions can be based on either the username, certificate, user information returned by the realm's directory server, or other administrator defined criteria.

The high-level configuration workflow is as follows:

1. Configure the Authentication Server
2. Configure User Roles
3. Configure Restrictions

4. Configure Authentication Realm
5. Configure Sign-in Policy

Sign-in Policy

Sign-in policies define the URLs that users and administrators use to access the device and connect to the network. This also provides option to the administrator to select the set of pages that users see during the sign-in process. Note that, these pages can be customized by using Custom Sign-in Pages option.

For example, if the enterprise has both PC users and mobile users, the admin can define two different URLs so that different authentication methods can be used. The ICS could log in to the IPS with an RSA token and their AD username and password. The mobile device use a client certificate (provided by an MDM solution) and the AD username and password.

User Roles

The user can be assigned to one or more roles during the sign-in process. A role is an entity which defines user session settings, role restrictions, appearance of the welcome page, and type of access methods (Pulse Client or agentless).

Creating Roles

To create a user role:

1. Select **Users > User Roles**. For creating Administrator role, select **Administrators > Admin Role**.

An administrator role specifies system management functions and session properties for administrators who map to the role. You can customize an administrator role by selecting the feature sets and user roles that members of the administrator role can view and manage.

2. Click **New Role** and then enter a name and, optionally, a description. This name is displayed in the list of Roles on the Roles page.

- Under Options, specify the session and appearance details.
 - Session Options**—Sets timeouts and user permissions that apply to each session established through the role.
 - UI Options**—Sets the appearance of agentless log in pages.
 - Guest User Account Management**—Provides limited permissions to allow users assigned to this role to create guest accounts

User Roles > New Role

New Role

Name:

Description:

▼ Options

Session and appearance options are specified in [Default Options](#). Check the following if this role should override these defaults.

- Session Options
- UI Options
- Odyssey Settings for Access
- Odyssey Settings for Preconfigured Installer
- Enable Guest User Account Management Rights
- Enable Sponsored Guest User Account Management Rights

[Save Changes](#)

Configuring User Access Options

IPS supports connection through an agent (software) installed on the client device. The supported agent type is Pulse Client. The Administrator can configure what agent to install on the client device and the corresponding settings to push during the installation.

To configure the user access options:

1. Select **Users > User Roles > Role Name > Agent**.

The screenshot shows the configuration page for a user role named 'Agent'. The breadcrumb trail is 'User Roles > Users > Agent > General'. The 'Agent' tab is selected. Under the 'Options' section, the 'Install Agent for this role' checkbox is checked, and the 'Install Pulse Secure client' radio button is selected. The 'Enable Host Enforcer' checkbox is unchecked. Below this, there is a note about Host Enforcer policies and a link to 'Access control'. Under the 'Session scripts' section, there are two fields for 'Script Location': 'Windows: Session start script' and 'Windows: Session end script'. A 'Save Changes' button is at the bottom.

2. To allow Pulse to download automatically on Windows endpoints, select Install Agent for this role, and then select the Install **Pulse Client** option.
3. Under **Session Scripts**, specify scripts to run on Windows endpoints for users assigned to a role. For example, you can specify a script that maps network drives on an endpoint as a session start script, and you can specify another script that disconnects the mapped network drives as session end script.

Customizing UI Options

IPS provides options to administrators in customizing the page that gets displayed to the end users during sign-in process. These customization options are applied based on the list of user roles that are getting assigned to the end user. Using these options, administrators can change the logo, background and the welcome message that gets displayed to the end users during the sign-in process.

To customize the welcome page:

1. Select **Users > User Roles > Role Name > General > UI Options**.

The screenshot shows the 'UI Options' configuration page for a user role. The page is divided into several sections:

- Current appearance:** Shows the current logo as 'Pulse Secure'. There is a 'Browse' button to change the logo image and a 'Background color' field with a color palette icon. The current color is '#993333'.
- User toolbar:** Includes a 'Session Counter' checkbox.
- Post Auth Sign-In Notification:** Includes a dropdown menu for '(None)' and a 'Show notification message on user's welcome page' checkbox.
- Informative:** Includes a 'Show instruction message' checkbox with a text area containing a sample message: 'Welcome to the Pulse Policy Secure. Do not navigate away from this page, or you will lose access to protected resources.'
- User Admin:** Includes a 'Show User Admin Instruction message' checkbox with a text area and an 'Enable bulk user creation' checkbox.
- Other:** Includes a 'Show copyright notice and "Secured by Pulse Secure" label in footers' checkbox.

Buttons for 'Save Changes' and 'Restore Factory Defaults' are located at the top and bottom of the page.

2. (Optional) **Under Header**, specify a custom logo and alternate background color for the header area of the welcome page:

- Click **Browse** and locate your custom image file. The new logo is displayed in the **Current appearance** box only after you save your changes.
- Type the hexadecimal number for the background color, or click the Color Palette icon and select a color. The Current appearance box updates immediately.

3. Under **User Toolbar**, select the Session Counter check box to display both a session countdown timer and an Extend button that allows agentless users to extend their session time to the maximum session length if the Enable Session Extension option is selected.

4. (Optional) Under **Post-Auth Sign-In Notification**, select a post authentication message that you configured earlier. If you select this option, the user receives an information page (for example, an end-user license agreement [EULA]) that you have created.

5. (Optional) Under **Personalized greeting**, select the Show notification message check box, and enter a message in the associated text box. The message is displayed as a header on the welcome page after the user is authenticated. You can format text and add links using the following HTML tags: `<i>`, ``, `
`, ``, and `<a href>`. This information does not appear on the initial sign-in page that is displayed prior to authentication. You can also use system variables and attributes in this field. The length of the personalized greeting cannot exceed 12K, (12288 characters). If you use unsupported HTML tags in your custom message, the system might display the user's home page incorrectly.
6. (Optional) Under **Informative**, select the Show instruction message check box and specify any instructions to appear on the welcome page. For example, you could advise users of company privacy notices or usage restrictions, or you can link to another site for more information.
7. If you include a link to an external website, a warning message appears informing the user of loss of access privileges if they leave the current page. To avoid this, add a tag for opening links in a new browser window.

For example: `Google` displays the linked text "Google," and the link opens in a new browser window.

The instruction message supports non-English languages.

8. (Optional) Under **User Admin**, select the Show User Admin instruction message checkbox and specify any instructions to appear on the user admin page. Select Enable bulk user creation to create bulk user accounts for numerous users.
9. (Optional) Under **Other**, specify whether to display the copyright notice and label in the footer. This setting applies only to users whose license permits disabling the copyright notice. For more information about this feature, call Ivanti Support.
10. (Optional) Click **Restore Factory Defaults** to reset all user-interface options back to factory defaults.
11. Click **Save Changes**.



- If a user maps to more than one role, then the system displays the user interface settings that correspond to the first role to which the user is mapped.
 - Sign-in pages can also be customized using the Custom Sign-In page functionality. For more information, see [Configuring Custom Sign-In Pages](#)
-

Customizing the Session Options

IPS provides option to administrators for configuring the maximum session length and heartbeat interval for the end user sessions. Using these options Administrator can control how long the user sessions are allowed and the interval within which server should receive heartbeat from client device.

IPS also provides option to enable session roaming so that mobile users can continue to have the connection with server while roaming.

To specify general session options:

1. Select **Users > User Roles > RoleName > General > Session Options**.

The screenshot displays the 'Session Options' configuration page. It features a top navigation bar with 'General', 'Agent', and 'Agentless' tabs. Below this is a sub-navigation bar with 'Overview', 'Restrictions', 'Session Options', and 'UI Options'. A 'Save Changes' button is located at the top left. The main content area is divided into sections: 'Session lifetime' with input fields for 'Max. Session Length' (725 minutes), 'Heartbeat Interval' (900 seconds), 'Heartbeat Timeout' (1800 seconds), and 'Auth Table Timeout' (60 seconds); 'Enable session timeout warning' with radio buttons for 'Enabled' and 'Disabled' (selected); and 'Roaming session' with radio buttons for 'Enabled (maximize mobility)', 'Limit to subnet (some mobility, increased security)', and 'Disabled (maximize security)'. A 'Save Changes' button is at the bottom left.

2. For **Max. Session Length**, specify the number of minutes an active non-administrative user session can remain open before ending. The minimum is 6 minutes. The maximum is 725 minutes. During a user session, prior to the expiration of the maximum session length, the system prompts the user to reenter authentication credentials, thereby avoiding the unexpected termination of the user session.

3. For **Heartbeat Interval**, set the frequency at which the endpoint sends out a heartbeat to IPS to keep the session alive. For agentless access, the browser refreshes the page with every heartbeat. Users must not the browser, because this will interrupt the heartbeat and end the session. Pulse Client and the Java agent provide the heartbeat. You should ensure that the heartbeat interval of the agent is greater than the Host Checker interval. If it is not, performance could be affected. In general, set the heartbeat interval to 50% more than the Host Checker interval.
4. For Heartbeat Timeout, specify the amount of time the system should "wait" before terminating a session when the endpoint does not send a heartbeat response.
5. For Auth Table Timeout, enter a timeout value for the auth table entry to be provisioned as needed. This parameter allows you to specify how long a user with no activity (for example, a user reading a static web page), can remain in the auth table before the auth table entry is cleared by the Infranet Enforcer.
6. Enter the reminder time in minutes.
7. Guest users (users created by guest user account managers) can log in with their guest account, and then tunnel into their corporate Virtual Private Network (VPN). In this case, the heartbeat connection to IPS is lost, and the user is disconnected after the heartbeat timeout expires. To prevent this, use firewall traffic as the heartbeat by selecting the **Allow VPN Through Firewall** check box.



When the "Disable use of **Allow VPN Through Firewall** check box is not checked (the default setting), AJAX requests are sent to the IPS at the configured interval. If the Use Traffic as Heartbeats option is enabled, AJAX heartbeat errors are masked.

If a guest user is assigned two roles, and one of the roles has a Host Checker policy and one doesn't, the user loses the role with the Host Checker policy if the Host Checker policy expires while the user is accessing a VPN through a tunnel. The user will lose access to the resources associated with the Host Checker role.

8. For agentless users, you can select the **Enable Session Extension** check box to allow users with a Layer 2 or Layer 3 connection to continue a session beyond the maximum session length.

If this feature is enabled, users with agentless access can be reauthenticated and extend their current session without interruption.

When the user session nears the end of maximum session length, a pop up a new sign-in page for agentless. When the user enters credentials, Host Checker verifies that the user is still compliant and the session continues.

When the user extends the session before its expiration, the session time is restored to the original maximum session length time that you have specified for the role, and the log indicates the new session time. If the user fails to extend the session before session time expires, the session is terminated.

For agentless access, you must select the Session Counter option on the UI Options tab to enable the session timer.

9. Under Enable Session timeout warning, specify:

- **Enabled**-To enable expiration warning for users using Pulse Client.
- **Disabled**-To disable expiration warning message.

10. Under Roaming session, specify:

- **Enabled**-To enable roaming user sessions for users mapped to this role. A roaming user session works across source IP addresses, which allows mobile users (laptop users) with dynamic IP addresses to sign in from one location and continue working from another. Disable this feature to prevent users from accessing a previously established session from a new source IP address. This prevents the spoofing attack on the user's session.
- **Limit to subnet**-To limit the roaming session to the local subnet specified in the Netmask box. Users may sign in from one IP address and continue using their sessions with another IP address if the new IP address is within the same subnet.
- **Disabled**-To disable roaming user sessions for users mapped to this role. Users who sign in from one IP address may not continue an active session from another IP address. User sessions are tied to the initial source IP address.



You must enable roaming for roles that are created for security policies that classify sessions into VLANs, for example, VLANs that have been provisioned for Users or Remediation. A session stores the client IP address. If the session gets placed in a different VLAN transition, the control channel is re-established, and a new IP address is sent to the server. If the remediation role does not have roaming enabled, the server terminates the session. This can lead to repeated problems. When the session is terminated, it causes a new log on, which reconnects to the same session, resulting in the same roaming problem. The Pulse client sets a connection roaming error and logs the server FATAL_ERROR message.

11. Click **Save Changes**.

Configuring Role Restrictions

The role restrictions allow only a valid user to access the network and prevents unauthorized access. You can specify security requirements based on source IP address, password, certificate, browser type, and Host Checker policies. If the user does not meet the requirements specified in the restriction, then the user is not allowed to access the protected resource.

Source IP Access Restriction

Use a source IP restriction at the role to control from which IP addresses users can access a sign-in page. You must specify one or more IP addresses otherwise; no IP address restriction applies.

To enable Source IP access restriction:

1. Select **Users > User Roles > Select Role > General > Restrictions > Source IP**.
2. Assign the Source IP restrictions on roles.
 - **Allow users to sign-in** from any IP address- You can allow or deny access to any IP address/netmask combination. For example, you can deny access to all users on a wireless network (10.64.4.100), or you can allow access to all other network users (0.0.0.0).
 - **Allow or deny users from following IP address**- Enter the IPv4/IPv6 address, network/prefix length and choose whether to allow or deny access. Click **Add**.
3. Click **Save Changes**.

Certificate Access Restriction

Certificate access restriction restricts access only to clients that have a client-side certificates. You can further restrict access using specific certificate attribute and value pairs.

To enable certificate access restriction:

1. Select **Users > User Roles > Select Role > General > Restrictions > Certificate**.
2. Select the **Only allow users with a client certificate signed by Certificate Authority (CA)**.

3. Create a field/value pair check based on attributes within the client certificates. Enter the "Certificate field" and the expected value. Click **Add**. The value in the field depends on the naming attributes in the Relative Distinguished Name(RDN) in the subject DN of the certificate.

For example, if the subject DN is cn=user1, uid=uid1, sn=lastname, E=user1@sample.net, OU=QA, O=company, C=US, you can use 'cn', 'uid', 'sn', 'E', 'ou', 'o', 'c'.

4. Click **Save Changes**.

The screenshot shows the 'Certificate' configuration page for a role. The breadcrumb trail is 'User Roles > Full Access > General > Restrictions > Certificate'. The page has tabs for 'General', 'Agent', and 'Agentless', with 'General' selected. Below the tabs are sub-sections: 'Overview', 'Restrictions', 'Session Options', and 'UI Options', with 'Restrictions' selected. Under 'Restrictions', there are sub-sections: 'Source IP', 'Browser', 'Certificate', and 'Host Checker', with 'Certificate' selected. The main content area contains two radio button options: 'Allow all users (no client-side certificate required)' (selected) and 'Only allow users with a client-side certificate signed by Certification Authority to sign in. To change the certification authority, see the Trusted Client CA page. Important: To enable certificate restrictions or conditions for this role, you must first choose to remember certificate information or enable certificate restrictions at the realm(s) that map users to this role, see Users Authentication page.' Below these options is a section titled 'You can optionally require specific values in the client certificate:' with a dropdown menu set to '10 records per page' and a search box. A table with two columns, 'Certificate field (example "cn")' and 'Expected value', is present. The table is currently empty. An 'Add' button is located to the right of the table. At the bottom left is a 'Save Changes' button, and at the bottom right are navigation buttons: '← Previous', '1', and 'Next →'.

Host Checker Restrictions

To specify Host Checker restrictions:

1. Select **Users > User Roles > Select Role > General > Restrictions > Host Checker**.
2. Select **Allow only users whose workstations meet the requirements specified by these Host Checker policies** to apply HC restrictions.
3. Select the Host Checker policy from the Available Policies list and click **Add**.
4. Select the Allow access to role if any ONE of the selected policies is passed check box if you do not want to require users to meet all of the requirements in all of the selected policies.
5. Click **Save Changes**.

User Roles > Full Access Role > General > Restrictions > Host Checker

Host Checker

General Agent Agentless

Overview Restrictions Session Options UI Options

Source IP Browser Certificate Host Checker

Allow all users (Host Checker not required)

Allow users whose workstations meet the requirements specified by these Host Checker policies:

Available Policies: Selected Policies:

antivirus Add -> Notepad

Remove

Allow access to the role if any ONE of the selected policies is passed.

To manage Host Checker policies, see the [Host Checker](#) configuration page.

Save Changes

Browser Restriction

To specify browser restrictions:

1. Select **Users > User Roles > Select Role > General > Restrictions > Browser**.
2. Select **Only allow users matching the following user-agent policy** to define browser access control rules.

3. To create a rule:

- For the user-agent string pattern, enter a string in the format `*<browser_string>*`
where asterisk (*) is an optional character used to match any character and `<browser_string>` is a case-sensitive pattern that must match a substring in the user-agent header sent by the browser. You cannot include escape characters (\) in browser restrictions.
- Select either:
 - **Allow** to allow users to use a browser that has a user-agent header containing the `<browser_string>` substring.
 - **Deny** to prevent users from using a browser that has a user-agent header containing the `<browser_string>` substring.
- Click **Add**.

4. Click **Save Changes**.

Rules are applied in order, so the first matched rule applies. Literal characters in rules are case sensitive, and spaces are allowed as literal characters. For example, the string `*Opera*` matches any user-agent string that contains the substring Opera.

The screenshot shows the configuration page for Browser Restrictions. The breadcrumb trail is "User Roles > Full Access Role > General > Restrictions > Browser". The page title is "Browser". There are three tabs: "General", "Agent", and "Agentless", with "General" selected. Below the tabs are four sub-sections: "Overview", "Restrictions", "Session Options", and "UI Options", with "Restrictions" selected. Under "Restrictions", there are three sub-sections: "Source IP", "Browser", and "Certificate", with "Browser" selected. The main content area has two radio buttons: "Allow all users matching any user-agent string sent by the browser." (selected) and "Only allow users matching based on the user-agent string sent by the browser. Note that some browsers allow users to change this string, so this is not a guaranteed method of identifying the browser type." Below the radio buttons are "Delete", "Up", and "Down" buttons. A table with one row is visible, with columns for "User-agent" and "Access". The "User-agent" column has an input field, and the "Access" column has "Allow" (selected) and "Deny" radio buttons. At the bottom, there is a note: "Note: This restriction will not allow access to the role if no user-agent strings are listed." and a "Save Changes" button.

User-agent	Access
<input type="text"/>	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

Authentication Realm

An authentication realm defines the authentication server with which end user is authenticated and the list of restrictions that must be satisfied on the client machine during sign-in. It also provides role mapping option to administrators for configuring the list of roles that needs to be assigned to the user. Role mapping provides flexibility to administrators in configuring how different set of roles need to be assigned to the user.

Creating an Authentication Realm

To create an authentication realm:

1. Select **Administrators > Admin Realms or Users > User Realms**.
2. On the respective Authentication Realms page, click **New**.

User Realms > New Authentication Realm

New Authentication Realm

* Name: Label to reference this realm

Description:

When editing, start on the Role Mapping page

▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Specify the server to use for authenticating users.

User Directory/Attribute: Specify the server to use for authorization.

Accounting: Specify the server to use for Radius accounting.

Device Attributes: Specify the server to use for device authorization.

▼ Additional Authentication Server

Enable additional authentication server

▼ Dynamic policy evaluation

Enable dynamic policy evaluation

* indicates required field

3. Enter a name to label this realm and, optionally, a description.
4. Select **When editing, start on the Role Mapping page** if you want the Role Mapping tab to be selected when you open the realm for editing.

5. Under Servers, specify:
 - An authentication server to use for authenticating users who sign in to this realm.
 - (Optional) A directory/attribute server to use for retrieving user attribute and group information for role-mapping rules and resource policies.
 - (Optional) A RADIUS accounting server to use to track when a user signs in and out.
 - Device attributes server to use the device attributes.
6. If you previously selected a RADIUS server for Authentication, the RADIUS Proxy option buttons appear. Select **Proxy Outer Authentication or Proxy Inner Authentication** to allow the system to proxy EAP authentication methods. Select **Do not proxy** if you do not want to use RADIUS proxy.
7. Select Enable additional authentication server to specify an additional authentication server.

8. To use dynamic policy evaluation for this realm, select **Dynamic policy evaluation** to enable an automatic timer for dynamic policy evaluation of this realm's authentication policy, role-mapping rules, and role restrictions. Then:
 - Select the **Refresh interval** option to specify how often to perform an automatic policy evaluation of all currently signed in realm users. Specify the number of minutes (5 to 1440).
 - Select **Refresh roles** to refresh the roles of all users in this realm. (This option does not control the scope of the Refresh Now button.)
 - Select **Refresh resource policies** to also refresh the resource policies (not including Meeting and e-mail Client) for all users in this realm. (This option does not control the scope of the Refresh Now button.)
 - Click **Refresh Now** to manually evaluate the realm's authentication policy, role-mapping rules, role restrictions, user roles, and resource policies of all currently signed-in realm users. Use this button if you make changes to an authentication policy, role-mapping rules, role restrictions, or resource policies and you want to immediately refresh the roles of this realm's users.
 - To use session migration for endpoints with the Pulse client, select the **Session Migration** check box. Then enter the Authentication Group and specify whether you want to receive user attributes from IF-MAP or from a directory server. Note that you must also configure IF-MAP Federation for all of IPS nodes in a session migration network.
 - Click **Save Changes** to create the realm. The General, Authentication Policy, and Role Mapping tabs for the authentication realm appear.

9. Perform the next configuration steps:
 - Configure one or more role-mapping rules.
 - Configure an authentication policy for the realm.
 - After you configure the authentication realm, select **Authentication > Signing In > Signin Policies**, add the realm to a sign-in policy, and associate the realm with an authentication protocol set.

Configuring Admin/User Realm to associate an additional Authentication Server

To configure a user realm:

1. Select **Users > User Realms > New User Realm**.
2. Complete the settings for the user-realm.
3. Under **Additional Authentication Server**, select the **Enable additional authentication server** option.
4. Select any already created authentication-server from the Authentication #2 dropdown.
5. Specify the username and password.
 - Username: Specified by user on the sign-in page/Predefined as <USER>.



Configure Predefined as <NTUSER> if Primary Authentication server is AD server.

- Password: Specified by user in sign-in page options/Predefined as <PASSWORD>/Mask static password.
6. Click **Save Changes**.

Name: Label to reference this realm

Description:

When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Specify the server to use for authenticating users.

User Directory/Attribute: Specify the server to use for authorization.

Accounting: Specify the server to use for Radius accounting.

Device Attributes: Specify the server to use for device authorization.

Additional Authentication Server

Enable additional authentication server

You can specify an additional authentication server. The additional credentials can be specified by the user on the sign-in page (the labels for these inputs are specified by the sign-in page), or they can be pre-defined below, in which case the user will not be prompted for the credential.

Enable adaptive authentication

Note: Adaptive authentication is supported by leveraging the behavioral analytics. Enable behavioral analytics on 'System->Behavioral Analytics->Configuration' for supporting this. Adaptive Authentication is not supported with 'Anonymous' type authentication server selected as authentication server above.

Authentication #2:

Username is: specified by user on sign-in page
 predefined as:

Password is: specified by user on sign-in page
 predefined as: Mask static password

End session if authentication against this server fails



Certificate Auth Server and SQL Auth Server are currently not supported as secondary authentication server.

Configuring Realm Restrictions

Source IP Access Restriction

Use a source IP restriction at the realm to control from which IP addresses users can access a sign-in page.

To enable Source IP access restriction:

1. Select **Users > User Realm > Select Realm > Authentication Policy > Source IP**.
2. Select one of the following options:
 - **Allow users to sign-in** from any IP address- You can allow or deny access to any IP address/netmask combination. For example, you can deny access to all users on a wireless network (10.64.4.100), or you can allow access to all other network users (0.0.0.0).
 - **Allow or deny users from following IP address**- Enter the IPv4/IPv6 address, network/prefix length and choose whether to allow or deny access. Click Add.
3. Click **Save Changes**.

The screenshot shows the 'Source IP' configuration page under 'Authentication Policy'. It has two radio button options: 'Allow users to sign in from any IP address' (selected) and 'Allow or deny users from the following IP addresses'. Below the second option is a table with columns for 'IPv4/v6 Address', 'Netmask/Prefix Length', and 'Allow/Deny'. The 'Allow/Deny' column has 'Allow' selected and 'Deny' unselected. An 'Add' button is at the end of the table. A 'Delete' button and arrow icons are above the table. A note at the bottom states: 'Note: This restriction will not be enforced if no IP addresses are listed. Add one or more source IP addresses from which users are allowed to sign in or denied access.' A 'Save Changes' button is at the bottom left.

IPv4/v6 Address	Netmask/Prefix Length	Allow/Deny
<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
<input type="text"/>	<input type="text"/>	<input type="radio"/> Allow <input type="radio"/> Deny
<input type="text"/>	<input type="text"/>	<input type="radio"/> Allow <input type="radio"/> Deny

Certificate Access Restriction

Certificate access restriction restricts access only to clients that have a client-side certificates. You can further restrict access using specific certificate attribute and value pairs.

To enable certificate access restriction:

1. Select **Users > User Realms > Select Realm > Authentication Policy > Certificate.**
2. Select one of the following options:
 - **Allow all users-** Requires no client certificate.
 - **Allow all users and remember certificate information while user is signed in.**-Client certificate information is saved.
 - **Only allow users with a client certificate signed by Certificate Authority (CA).** – Requires client certificate signed by CA.
3. Create a field/value pair check based on attributes within the client certificates. Enter the "Certificate field" and the expected value. Click **Add**. The value in the field depends on the naming attributes in the Relative Distinguished Name(RDN) in the subject DN of the certificate. For example, if the subject DN is cn=user1, uid=uid1, sn=lastname, E=user1@sample.net, OU=QA, O=company, C=US, you can use 'cn', 'uid', 'sn', 'E', 'ou', 'o', 'c'.
4. Click **Save Changes**.

The screenshot shows the 'Certificate' configuration page under 'User Realms > Users > Authentication Policy > Certificate'. The page has tabs for 'General', 'Authentication Policy', and 'Role Mapping'. Under 'Authentication Policy', there are sub-tabs: 'Source IP', 'Browser', 'Certificate', 'Password', 'Host Checker', 'Limits', and 'RADIUS Request Policies'. The 'Certificate' tab is active, showing three radio button options:

- Allow all users (no client-side certificate required)
- Allow all users and remember certificate information while user is signed in.
- Only allow users with a client-side certificate signed by Trusted Client CAs to sign in. To change the certification authority, see the [Trusted Client CA](#) page.

 Below the options, there is a section titled 'You can optionally require specific values in the client certificate:' with a dropdown set to '10 records per page' and a search box. A table with two columns, 'Certificate field (example "cn")' and 'Expected value', is shown. The first row has empty input fields and an 'Add' button. At the bottom right of the table area, there are navigation buttons: '-- Previous', '1', and 'Next --'. A 'Save Changes' button is located at the bottom left of the form.

Host Checker Restrictions

To specify Host Checker restrictions:

1. Select **Users > User Roles > Select Realm > General > Restrictions > Host Checker**.
2. Select **Allow users whose workstations meet the requirements specified by these Host Checker policies** to apply HC restrictions.
3. Select the Host Checker policy from the Available Policies list and click Add.
4. Select the Allow access to role if any ONE of the selected policies is passed check box if you do not want to require users to meet all of the requirements in all of the selected policies.
5. Click **Save Changes**.

User Roles > Full Access Role > General > Restrictions > Host Checker

Host Checker

General Agent Agentless

Overview Restrictions Session Options UI Options

Source IP Browser Certificate Host Checker

Allow all users (Host Checker not required)

 Allow users whose workstations meet the requirements specified by these Host Checker policies:

Available Policies: Selected Policies:

antivirus

Allow access to the role if any ONE of the selected policies is passed.

To manage Host Checker policies, see the [Host Checker](#) configuration page.

Browser Restriction

To specify browser restrictions:

1. Select **Users > User Realms > Select Realm > Authentication Policy > Browser**.
2. Select **Only allow users matching the following user-agent policy** to define browser access control rules. To create a rule:
 - For the user-agent string pattern, enter a string in the format `*<browser_string>*` where asterisk (*) is an optional character used to match any character and `<browser_string>` is a case-sensitive pattern that must match a substring in the user-agent header sent by the browser. You cannot include escape characters(\) in browser restrictions.
 - Select one of the following options:
 - **Allow to allow users to use a browser that has a user-agent header** containing the `<browser_string>` substring.
 - **Deny to prevent users from using a browser that has a user-agent header** containing the `<browser_string>` substring.
 - Click **Add**.
3. Click **Save Changes**. Rules are applied in order, so the first matched rule applies. Literal characters in rules are case sensitive, and spaces are allowed as literal characters. For example, the string `*Opera*` matches any user-agent string that contains the substring Opera.

The screenshot shows the configuration page for the 'Browser' authentication policy. The 'Authentication Policy' tab is active, and the 'User-agent string pattern' section is expanded. The 'Allow/Deny' section is set to 'Allow'. The 'User-agent string pattern' field is empty, and the 'Add' button is visible. A note at the bottom states: 'Note: This restriction will not be enforced if no user-agent strings are listed. Once enforced the default policy is "deny all". Use wildcard "*" to add generic allow/deny policies.'

User Realms > Users > Authentication Policy > Browser

Browser

General Authentication Policy Role Mapping

Source IP Browser Certificate Password Host Checker Limits RADIUS Request Policies

Allow all users matching any user-agent string sent by the browser.
 Only allow users matching the following User-agent policy. Note that some browsers allow users to change this string, so this is not a guaranteed method of identifying the browser type.

Delete ↑ ↓

User-agent string pattern	Allow/Deny	
<input type="text"/>	<input checked="" type="radio"/> Allow <input type="radio"/> Deny	Add

Note: This restriction will not be enforced if no user-agent strings are listed. Once enforced the default policy is "deny all". Use wildcard "*" to add generic allow/deny policies.

Save Changes

Password Access Restriction

You can restrict network and resource access by password-length when administrators or users try to sign in. The user must enter a password whose length meets the minimum password-length requirement specified for the realm. Note that local user and administrator records are stored in the local authentication server. This server requires that passwords are a minimum length of 6 characters, regardless of the value you specify for the realm's authentication policy.

To specify password restrictions:

1. Select **Users > User Realms > Select Realm > Authentication Policy > Password**.
2. Select one of the following options:
 - **Allow all users (passwords of any length)** — Does not apply password restrictions on password length.
 - **Only allow users that have passwords of a minimum length** — Requires the user to enter a password with a minimum length that you specify.
3. Select **Enable Password Management** to enable password management. You must also configure password management on the authentication server configuration page (local authentication server) or through an LDAP server.
4. Select **Allow MS-CHAPv2 for Password authentication** to perform password authentication using MS-CHAPv2 protocol to allow single sign-on for Windows desktop clients.

- Click **Save Changes**. By default, the system requires that user passwords entered on the sign-in page be a minimum of four characters. The authentication server used to validate a user's credentials might require a different minimum length. For example, the local authentication database requires user passwords to be a minimum length of six characters.

The screenshot shows the configuration page for Password authentication. The breadcrumb trail is "User Realms > Users > Authentication Policy > Password". The page has tabs for "General", "Authentication Policy", and "Role Mapping". Under "Authentication Policy", there are sub-tabs for "Source IP", "Browser", "Certificate", "Password", "Host Checker", "Limits", and "RADIUS Request Policies". The "Password" sub-tab is active. The main content area is titled "Options for primary authentication server" and contains the following settings:

- Allow all users (passwords of any length)
- Only allow users that have passwords of a minimum length:
 - Minimum Length: characters
- Enable Password Management
 - This option enables the device to relay vital password information to users and enables users to change their passwords.
 - Note: You must also configure password management on the [Local Authentication server configuration page](#)
- Allow MS-CHAPv2 for Password Authentication
 - This option enables the device to perform password verification using the MS-CHAPv2 protocol. This allows single sign-on from Windows Desktop clients.

A "Save Changes" button is located at the bottom left of the configuration area.

Limits

To limit the number of simultaneous sessions:

- Select **Users > User Realms > Select Realm > Authentication Policy > Limits**.
- To limit the number of concurrent sessions, select the check box for Limit number of concurrent sessions, and type either a Guaranteed minimum and/or Guaranteed maximum.
- To limit the number of sessions for users, select Limit the number of concurrent sessions for users.
- Specify the number of sessions permitted for users in the Session Limit text box. By default, the number is 1 if the realm maximum is greater than 0; otherwise, the default is 0. The maximum number must be no greater than the maximum number of concurrent users for the realm.

- Click **Save Changes**.

User Realms > Users > Authentication Policy > Limits

Limits

General Authentication Policy Role Mapping

Source IP Browser Certificate Password Host Checker Limits RADIUS Request Policies

Limit number of concurrent sessions

Guaranteed minimum: 0 to realm maximum limit or maximum licensed sessions.

Maximum: guaranteed minimum to maximum licensed sessions.
Note: value "0" disables all logins to this realm.

Limit the number of concurrent sessions per user

Session limit: 1 to realm maximum.
Note: default value is 1 if realm maximum is > 0; otherwise default is 0.

Save Changes

RADIUS Request Policies

You can create RADIUS request attribute policies to require authentication requests to contain specific RADIUS attribute values. If an endpoint attempts to access a realm with a RADIUS request attribute policy, the endpoint must meet the conditions specified in the policy.

To add a RADIUS request attribute policy to a realm:

- Select a user realm on which you want to implement a RADIUS request attributes policy by selecting **Users > User Realms > Select Realm > Authentication Policy > RADIUS Request Policies**.
- Click **Add** to populate the Selected RADIUS Request Attributes Policies list from the available RADIUS Request Attribute Policies. The RADIUS request policies selected must be passed to allow users to access a realm. To configure RADIUS request policies, see [here](#).
- Select the Allow access to realm if any ONE of the selected policies are passed check box if you would like to allow access if any one of the selected policies is passed.

4. Click **Save Changes**.

The screenshot shows the 'RADIUS Request Policies' configuration page. The breadcrumb trail is 'User Realms > Users > Authentication Policy > RADIUS Request Policies'. The page has three tabs: 'General', 'Authentication Policy' (which is active), and 'Role Mapping'. Below the tabs are several sub-sections: 'Source IP', 'Browser', 'Certificate', 'Password', 'Host Checker', 'Limits', and 'RADIUS Request Policies' (which is also active). A descriptive text states: 'Restrict the users based on the RADIUS request attributes received from the connecting NAS device. If none of these policies are set then all users will be allowed. By default, a user will be allowed if any one of the selected policies holds true. To configure these policies go to RADIUS Request Policies.' The main configuration area is divided into two columns: 'Available RADIUS Request Attribute Policies:' and 'Selected RADIUS Request Attribute Policies:'. The 'Available' column contains '(none)'. The 'Selected' column contains 'Radius request policy'. Between these columns are 'Add ->' and 'Remove' buttons. Below the columns is a checkbox labeled 'Allow access to realm if any ONE of the selected policies are passed', which is currently checked. At the bottom left of the form is a 'Save Changes' button.

Configuring Role Mapping

Role-mapping rules are conditions a user must meet to map to user roles.

To specify role-mapping rules for an authentication realm:

1. Select **Administrators > Admin Realms, Users > User Realms**.
2. Select a realm and then click the **Role Mapping** tab.

3. Click New Rule to access the Role Mapping Rule page. This page provides an inline editor for defining the rule.

User Realms > dot1x > Role Mapping > Role Mapping Rule

Role Mapping Rule

Rule based on: Username

* Name:

▼ Rule:if username...

is If more than one username should match, enter one username per line. You can use * wildcards.

▼ then assign these roles

Available Roles: dot1x, Guest, Guest Admin, pulse, remind

Selected Roles: (none)

Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

4. In the Rule based on list, select one of the following:

- **Username**—The system username entered on the sign-in page. Select this option if you want to map users to roles based on their usernames. If this is a RADIUS realm, and you are using RADIUS proxy for outer authentication, you cannot configure a role-mapping rule with a username.
- **User attribute**—A user attribute from a RADIUS, LDAP, or SiteMinder server. Select this option if you want to map users to roles based on an attribute from the corresponding server. This type of rule is available only for realms that use a RADIUS server for the authentication server, or that use an LDAP or SiteMinder server for either the authentication server or the directory server. After choosing the User attribute option, click **Update** to display the Attribute list and the Attributes button. Click the **Attributes** button to display the server catalog.
- **Certificate or Certificate attribute**—Certificate or Certificate attribute is an attribute supported by the users' client-side certificate. Select this option to map users to roles based on certificate attributes. The Certificate option is available for all realms. The Certificate attribute option is available only for realms that use LDAP for the authentication or directory server. After choosing this option, click Update to display the Attribute text box.
- **Group membership**—Group membership is group information from an LDAP or native Active Directory server that you add to the server catalog Groups Tab. Select this option to map users to roles based on either LDAP or Active Directory group information. This type of rule is available only for realms that use an LDAP server for either the authentication server or directory server or that use an Active Directory server for authentication. (Note that you cannot specify an Active Directory server as an authorization server for a realm.)
- **Custom Expressions**—Custom Expressions is one or more custom expressions that you define in the server catalog. Select this option to map users to roles based on custom expressions. This type of rule is available for all realms. After you select this option, click Update to display the Expressions lists. Click the Expressions button to display the Expressions tab of the server catalog.
- **Anomaly Attribute**-Select this option for behavioral analytics.

5. Under Rule, specify the condition to evaluate, which corresponds to the type of rule you select and consists of the following:
 - If you are creating a role mapping rule for a MAC address authentication realm, the attributes list cannot be edited. If there is an LDAP server assigned to this MAC authentication server and you want to use and edit the attributes assigned to that LDAP server, please specify the LDAP server as the Directory/Attribute server.
 - Specifying one or more usernames, SiteMinder user attribute cookie names, RADIUS or LDAP user attributes, certificate attributes, LDAP groups, or custom expressions.
 - Specifying to what the value must equate, which might include a list of usernames, user attribute values from a RADIUS, SiteMinder, or LDAP server, client-side certificate values (static or LDAP attribute values), LDAP groups, or custom expressions.

For example, you can choose a SiteMinder user attribute cookie named "department" from the Attribute list, choose is from the operator list, and then enter "sales" and "eng" in the text box.

Alternatively, you can enter a custom expression rule that references the SiteMinder user attribute cookie named department:

<userAttr.department = ("sales" and "eng")>

6. Under **then assign these roles**:
 - Specify the roles to assign to the authenticated user by adding roles to the Selected Roles list.
 - Select **Stop processing rules when this rule matches** if you want the system to stop evaluating role-mapping rules if the user meets the conditions specified for this rule.
7. Click **Save Changes** to create the rule on the Role Mapping tab. When you finish creating rules, be sure to order role-mapping rules in the order in which you want the system to evaluate them. This task is particularly important when you want to stop processing role-mapping rules when a match is identified.

User Role Evaluation

Administrator can configure the role mapping rules for determining the list of roles that need to be assigned to the users. In case of multiple role assignment, IPS merges the various role settings using permission merge. Administrators can also configure how different rules can be evaluated and merged using the options provided on role mapping rules page.



If you assign a role to a RADIUS proxy realm, role restrictions cannot be enforced. Host Checker policies, source IP restrictions, and any other limits that have been assigned are bypassed. Use RADIUS proxy only if no restrictions have been applied. Additionally, outer proxy cannot be used if a role-mapping rule based on usernames is being used, because the system cannot see the username, and a session cannot be created.

A permissive merge is a merge of two or more roles that combines enabled features and settings according to the following guidelines:

- Any enabled access feature in one role takes precedence over the same feature set to disabled in another role. For example, if a user maps to two roles, one of which disables the Host Enforcer while the other role enables the Host Enforcer, the system enables the Host Enforcer for that session.
- In the case of user interface options, the system applies the settings that correspond to the user's first role.
- In the case of maximum session lengths, the system applies the greatest value from all the roles to the user's session.
- If more than one role enables the Roaming Session feature, then the system merges the netmasks to formulate a greater netmask for the session

The system performs the following security checks before creating a session for a role:

1. The system begins rule evaluation with the first rule on the Role Mapping tab of the authentication realm to which the user successfully signs in. During the evaluation, the system determines if the user meets the rule conditions. If so, then:
 - The system adds the corresponding roles to a list of eligible roles available to the user.
 - The system determines if the "stop on match" feature is configured. If so, then the engine proceeds.
2. The system evaluates the next rule on the authentication realm's Role Mapping tab according to the process in Step 1 and repeats this process for each subsequent rule. When the system evaluates all role-mapping rules, it compiles a comprehensive list of eligible roles.

3. The system evaluates the definition for each role in the eligibility list to determine whether the user complies with any role restrictions. The system then uses this information to compile a list of valid roles, whose requirements the user also meets. If the list of valid roles contains only one role, then the system assigns the user to that role. Otherwise, the system continues the evaluation process.
4. The system evaluates the setting specified on the Role Mapping tab for users who are assigned to more than one role:
 - **Merge settings for all assigned roles**—If you select this option, the system performs a permissive merge of all the valid user roles to determine the overall (net) session role for a user session.
 - **User must select from among assigned roles**—If you select this option, the system presents a list of eligible roles to an authenticated user. The user must select a role from the list, and the system assigns the user to that role for the duration of the user session.
 - **User must select the sets of merged roles assigned by each rule**—If you select this option, the system presents a list of eligible rules to an authenticated user (that is, rules whose conditions the user has met). The user must select a rule from the list, and the system performs a permissive merge of all the roles that map to that rule.

If you use automatic (time-based) dynamic policy evaluation or if you perform a manual policy evaluation, the system repeats the role evaluation process described in this section.

Sign-in Policies

Sign-in policies define the URL's that any user needs to use for accessing the network. IPS provides support for sign-in URL's for administrators and end users. Administrators can login to IPS using the administrator sign-in URL and configure/monitor the server. The user's login using the user sign-in URL's for connecting to the network. The sign-in URL's are configured with authentication realm so that authentication of the users is performed during the sign-in process. Administrators can also use the custom sign-in pages on the sign-in URL's so that pages displayed for the users are customized.

Configuring Administrator Sign-In Policies

To configure administrator sign-in policy:

1. Select **Authentication > Signing In > Sign-in Policies**.
2. To create a new sign-in policy, click **New URL**. To edit an existing policy, click a **URL in the Administrator URLs or the User URLs** column.

3. To create an administrator sign-in policy, select the **Administrators** option button at the top of the page. (By default, the **Users** option button is selected.)
4. In the **Sign-in URL** field, enter the URL to associate with the policy. Use the format `<host>/<path>` where `<host>` is the hostname of IPS, and `<path>` is any string users must enter. For example: `users1.yourcompany.com/ic`. To specify multiple hosts, use the asterisk (*) wildcard character. For instance:
To specify that all administrator URLs must use the sign-in page, enter `*/admin`.



Use wildcard characters (*) only at the beginning of the hostname portion of the URL. The system does not recognize wildcards in the URL path.

5. (Optional) Enter a **Description** for the policy.

6. From the Sign-in Page list, select the page that you want to associate with the policy. You can select the default page, a variation of the standard sign-in page, or a custom page that you create using the customizable UI feature.
7. For administrator sign-in policies, under Authentication realm, specify which realm maps to the policy, and how users and administrators must choose from among realms. If you select:
 - **User types the realm name**—The system maps the sign-in policy to all authentication realms but does not provide a list of realms from which the administrator can choose. Instead, the administrator must manually enter the realm name into the sign-in page.
 - **User picks from a list of authentication realms**—The system maps the sign-in policy to only the authentication realms that you choose. The system presents this list of realms when the administrator signs in and allows a realm to be chosen from the list. (Note that the system does not provide a list of authentication realms if the URL is mapped only to one realm. Instead, only the realm you specify is displayed).
8. Click the **Add** button to add available realms to the Selected realms box.
9. Click **Save Changes**.

Configuring User Sign-In Policies

To create or configure user sign-in policies:

1. Select **Authentication > Signing In > Sign-in Policies**.
2. To create a new sign-in policy, click **New URL**. To edit an existing policy, click a **URL in the Administrator URLs or User URLs** column.

Signing in > Sign-in Policies > */certauth/

***/certauth/**

User type: Users Administrators

Sign-in URL: Format: <host>/<path>/; Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: To create or manage pages, see [Sign-In pages](#).

Authentication realm

Specify what realms will be available when signing in.

<input type="checkbox"/>	Available realms	Authentication protocol set	
	<input type="text" value="Cert Auth"/>	<input type="text" value="- Not applicable -"/>	<input type="button" value="Add"/>
<input type="checkbox"/>	Cert Auth	Cert Auth	

If more than one realm appears above, Odyssey Access Client or the Policy Secure sign-in page will ask the user to choose. Other endpoints cannot choose a realm; the Policy Secure will assign the first suitable realm from the list. If no realms appear above, sign-in will fail.

User may specify the realm name as a Username suffix
When this option is selected, the Username suffix will be used to specify a realm

Remove realm suffix before passing to authentication server
When this option is selected, the username suffix will be stripped from the Username prior to authenticating with an authentication server

Fail if suffix does not match any of the realms
When this option is selected, the user should provide one of the realm as suffix. If not, the user will be denied sign-in.

Configure Guest Settings

Use this signin policy for Guest and Guest admin to use specific pages.

Configure SignIn Notifications

Pre-Auth Sign-in Notification

Post-Auth Sign-in Notification

3. In the **Sign-in URL** field, enter the URL that you want to associate with the policy. Use the format `<host>/<path>`, where `<host>` is the host name of IPS, and `<path>` is any string users must enter. For example: `users1.yourcompany.com/ic`. To specify multiple hosts, use the asterisk (*) wildcard character. For example, to specify that all end-user URLs must use the sign-in page, enter `*/`.
4. Under **Authentication realm**, specify the realms that must be mapped to the sign-in policy. Under Available realms, select realms from the menu. The system maps the sign-in policy only to the authentication realms that you add.

5. Under **Authentication protocol set**, select an authentication protocol set that you have configured previously. If endpoints will connect with a IPS agent, select the default 802.1X protocol set. The protocol set used with a realm must be compatible with the authentication server that is associated with the realm.
6. Click **Add** to add the new realm and authentication protocol pair.
7. Select the **User may specify the realm name as a username suffix** check box to allow non- IPS endpoints to access the system by entering their credentials (in the format *user@realm*).
8. Select the **Remove realm suffix before passing to authentication server** check box for users to enter their credentials with a suffix to send the username without the suffix. Most authentication servers are not compatible with a realm suffix or decorated username.
9. Click **Save Changes**.

Associating Authentication Realms and Protocols with User Sign-in Policies

Different types of endpoints can request authentication through IPS, including IPS agents, third-party 802.1X supplicants (including 802.1X IP phones), switches, and endpoints that request authentication with agentless access.

A IPS agent is software that can use the JUAC protocol. IPS agents include Pulse Client client, and the Java agent. By default, IPS can communicate with IPS agents, the Java agent, and endpoints with agentless access. To accommodate other types of endpoint clients, you might need to create authentication protocol sets within sign-in policies.

When you add a realm in a sign-in policy, you select an authentication protocol set to be used with that realm. There are two default authentication protocol sets. For IPS agents, use the default 802.1X authentication protocol set. For 802.1X IP phones, use the default 802.1X-Phones protocol set.

Third-party 802.1X supplicants cannot use the preconfigured 802.1X protocol set that is used by default with IPS agents. For example, some switches can request authentication using CHAP or EAP-MD5-Challenge. You must define a specific authentication protocol set for these requests.

To define an endpoint's authentication method, you add authentication realms to sign-in policies. You configure authentication protocol sets as required, based on authentication methods that are compatible with the authentication server that you are using. IPS maps the sign-in policy to the authentication realms that you choose. Users who sign in using the URL that you provide have access only to those realms that you specify.

For non- IPS agents, you must select the protocols that the client and the authentication server are compatible with. See the below table for details of what authentication protocols are compatible with different authentication servers.

Protocols	Authentication Servers				
	Certificate	Local	Active Directory	ACE	Mac Auth
EAP-GTC	-	-	-	Y	-
PAP	-	Y	Y	Y	-
CHAP, EAP-MD5-Challenge	-	Y	-	-	-
MS-CHAP	-	Y	Y	-	-
MS-CHAP-V2, EAP-MS-CHAP-V2	-	Y	Y	-	-
EAP-TLS	Y	-	-	-	-
Mac-based auth		-	-	-	Y
EAP-JUAC	Y	Y	Y	Y	-



For 802.1X, AD authentication server used as LDAP is not supported for the following protocols: MS-CHAP, MS-CHAP-V2, and EAP-MS-CHAP-V2.

The decision of what realms are available to the user within a sign-in policy is based on two factors. First, the order of realms in the list is considered. Realms at the top of the list are attempted. Second, the authentication protocol set that you choose must be compatible with the client or supplicant.

To determine a compatible realm, the system looks for a RADIUS subprotocol that is compatible with the client or supplicant's available protocols, and the system automatically selects compatible realms. If the endpoint is using a Ivanti Policy Secure agent, the system presents a list of realms. Any realm with both outer and inner protocols that match the outer and inner protocols on the client is considered compatible.

Protocol compatibility does not guarantee authentication. For example, CHAP and EAP-MD-5 challenge sign-in succeeds only if the stored password is retrievable as clear text. In addition, if the client or supplicant is configured with a non-JUAC protocol (for example, the Windows Vista supplicant), the system searches for a realm without TNC Host Checker restrictions, browser restrictions, or certificate restrictions.



If you are configuring a realm for a Windows client, with a Statement of Health Host Checker policy, you must use an authentication protocol set with the EAP-SOH protocol. When you select EAP-SOH in an authentication protocol set, EAP-SOH is always offered first, regardless of protocol ordering.

If an endpoint is using IPS agent software, the system presents the list of realms to the user or administrator when the user signs in and allows the user to choose a realm from the list. The system does not display a list of authentication realms if the URL is mapped only to one realm. Instead, it automatically uses the realm you specify.

For endpoints that use a non-IPS agent, you can select the User may specify the realm name as a username suffix check box. When the user provides a username with a suffix in the format user@realm, the suffix determines the realm assignment. If you do not select this option, the endpoint is assigned to the first realm in the list whose authentication server is a match with the endpoint's software. For example, if the endpoint's software is configured for tokens (EAP-Generic Token Card), and if the sign in policy permits EAP-GTC, the endpoint is assigned the first realm in the list whose authentication server supports tokens.

When an 802.1X IP phone connects through a realm with the 802.1X-Phone protocol set selected, the device is automatically directed to the proper realm for authentication based on the compatible protocol.

If you are using inner or outer RADIUS proxy with a selected realm, routing with respect to authentication protocols is different. IPS forwards all traffic to a proxy target, which rejects protocols it does not support. With an outer proxy realm, IPS ignores the authentication protocol set. For an inner proxy realm, the authentication protocol set directs IPS as it negotiates the outer protocol (EAP-PEAP or EAP-TTLS) but does not affect the inner protocol.

Managing Sign-In Policies

This topic describes how to configure and manage user sign-in policies.

Enabling and Disabling Sign-in Policies

IPS provides an option to control the list of sign-in URL's that can be used by the users for logging into the network. The Administrator can control the list of sign-in URL's that are allowed for sign-in process using enable/disable functionality. Sign-in URLs that are disabled on Ivanti Policy Secure cannot be used by the users for connecting to the network.

To enable and disable sign-in policies:

1. Select **Authentication > Signing In > Sign-in Policies**.

Sign-in Policies

Restrict access to administrators only
Only administrator URLs will be accessible. Note that Administrators can attempt to sign in even if all rules on this page are disabled.
Warning: Enabling this option will immediately terminate all user sessions.

New URL... Delete... Enable Disable ↑ ↓ Save Changes

Administrator URLs	Sign-In Page	Authentication Realm(s)	Enabled
<input type="checkbox"/> */admin/	Default Sign-In Page	Admin Users	✓
User URLs	Sign-In Page	Authentication Realm(s)	Enabled
<input type="checkbox"/> */guestadmin/	Default Sign-In Page	Guest Admin (N/A)	✓
<input type="checkbox"/> */guest/	Default Sign-In Page	Guest (Guest)	✓
<input type="checkbox"/> */certauth/	Default Sign-In Page	Cert Auth (Cert Auth)	✓
<input type="checkbox"/> */	Default Sign-In Page	Users (802.1X)	✓

2. Select the check box for the policy that you want to change then click **Enable** or **Disable** for enabling or disabling an individual policy.
3. Select or clear the **Restrict access to administrators only** check box at the top of the page to enable or disable the policy or all user policies.
4. Click **Save Changes**.

Specifying the Order of Evaluation

The IPS evaluates sign-in policies in the same order that you list them on the Sign-in Policies page. When it finds a URL that matches exactly, it stops evaluating and presents the appropriate sign-in page to the administrator or user. For example, for 2 administrator sign-in policies with different URLs:

- The first policy uses the URL */admin and maps to the default administrator sign-in page.
- The second policy uses the URL yourcompany.com/admin and maps to a custom administrator sign-in page.

If you list the policies in this order on the Sign-in Policies page, the system never evaluates or uses the second policy because the first URL encompasses the second one. Even if an administrator signs in using the yourcompany.com/admin URL, the system displays the default administrator sign-in page. If you list the second policy first, however, the system displays the custom administrator sign-in page to administrators who access the system using the yourcompany.com/admin URL.

Note that the system accepts only wildcard characters in the hostname section of the URL and matches URLs based on the exact path. For example, two administrator sign-in policies with two different URL paths:

- The first policy uses the URL */marketing and maps to a custom sign-in page for the entire Marketing Department.
- The second policy uses the URL */marketing/joe and maps to a custom sign-in page designed exclusively for Joe in the Marketing Department.

If you list the policies in this order on the Sign-in Policies page, the system displays Joe's custom sign-in page to him when he uses the yourcompany.com/marketing/joe URL to access the system. He does not see the Marketing sign-in page, even though it is listed and evaluated first, because the path portion of his URL does not exactly match the URL defined in the first policy.

To change the order in which administrator sign-in policies are evaluated:

1. Select **Authentication > Signing In > Sign-in Policies**.
2. Select a sign-in policy in the **Administrator URLs or User URLs** list.
3. Click the up or down arrow to change the selected policy's placement in the list.

4. Click **Save Changes**.

Signing In > Sign-In Policies

Sign-in Policies

Sign-in Pages | Sign-in Notifications | Authentication Protocol Sets

Restrict access to administrators only
Only administrator URLs will be accessible. Note that Administrators can attempt to sign in even if all rules on this page are disabled.
Warning: Enabling this option will immediately terminate all user sessions.

New URL... Delete... Enable Disable **↑ ↓** Save Changes

Administrator URLs	Sign-In Page	Authentication Realm(s)	Enabled
<input type="checkbox"/> */admin/	Default Sign-In Page	Admin Users	✓
User URLs	Sign-In Page	Authentication Realm(s)	Enabled
<input type="checkbox"/> */guestadmin/	Default Sign-In Page	Guest Admin (N/A)	✓

Configuring Sign-In Notifications

With sign-in notifications, you can create and configure detailed notification messages that appear for Pulse clients and for agentless access endpoints when the user attempts to sign in. For example, you can configure a notification message that explains terms of use, company-specific policies, a welcome page, an end user license agreement (EULA), or a message of the day.

For a browser-based (agentless) log in, the notification message appears in a separate page either before (pre-auth) or after (post-auth) user authentication during the sign-in process. For a Pulse client log in, the notification messages appear in a Pulse message box. The user is expected to read the content of the sign-in notification message and acknowledge by clicking a Proceed button. The user may indicate disagreement by clicking a Decline button, which ends the log in attempt.

You can configure a sign-in policy to use a sign-in notification either as pre-auth or post-auth (or both). In the case of post-auth configuration, you can either use a common message for all roles or use separate messages for each role.

You can create a multi-language sign-in notification package that relies on the language setting of the endpoint. You can customize the sign-in notification page appearance for browser-based log ins by modifying the related fields in a sign-in page in the Admin UI or by using a custom sign-in page.

Configuring and Implementing Sign-In Notifications

Sign-in notifications appear for Pulse client and for browser-based logins when the user attempts to sign in.

To configure and implement sign-in notifications:

1. Select **Authentication > Signing In > Sign-in Notifications**.
2. Click **New Notification**.

Signing In > Sign-In Notification > New Sign-In Notification

New Sign-In Notification

Name: Label to reference the sign-in notification.

Type: Text Package

Text:

64 character(s)

Text for the sign-in notification.
NOTE: For Pulse desktop L3 VPN connections, the combined length of all the sign-in notification messages cannot exceed 3000 characters. If it does then the notifications will not be displayed to the user.

[Save Changes](#)

3. Specify a Name for the notification. This name appears in the sign-in policies page, and in the UI Options page for a selected role.
4. Select **Text** or **Package**.
 - If you select **Text**, type the desired sign-in notification message, or copy and paste the relevant text into the Text field.
 - If you select **Package**, click the **Browse** button and navigate to a previously prepared .zip file. A package is typically used to provide different language versions of the notification message.
 - The zip file should include a default.txt file and one or more <language>.txt files (Example: en.txt).
 - Language-abbreviations should be strings that can appear in Accept-Language header of an HTTP request.
 - The character encoding supported is UTF-tly.
5. Click **Save Changes**. To enable sign-in notifications:

6. Click **Authentication > Signing In > Sign-in Policies**.
7. Under Configure Sign-in Notifications, select the check box for **Pre-Auth Sign-in Notification**, **Post-Auth Sign-in Notification**, or both.
 - After Pre-Auth Sign-in Notification, select a previously configured sign-in notification from the drop-down menu.
 - After Post-Auth Sign-in Notification, select the option for **Use a common Sign-in Notification for all roles** or **Use the Sign-in Notification** associated to the assigned role.
 - If you select **Use a common Sign-in Notification for all roles**, select a previously configured sign-in notification from the drop-down menu.
 - If you select **Use the Sign-in Notification associated to the assigned role**, the sign-in notification configured for the assigned role will be used.
 - Prevent the Post-Auth sign-in notification from being displayed to users who have seen it before, by selecting the **Skip if already shown** check box. (This is only a hint to the system and might not be honored in all environments.)
8. Click **Save Changes**.
9. You can customize the appearance of the sign-in notification message by selecting **Authentication > Signing In > Sign-in Pages** and creating a sign-in page or using an existing page.

10. Under Sign-in Notification appearance, customize UI options for Pre-Auth Notifications and Post-Auth Notifications by changing the following items:
 - For **Notification Title** enter the text that appears at the top of the sign-in notification page.
 - In the **Proceed Button** box, enter the text for the button that the user clicks to proceed with the sign-in. This text applies to browser-based log ins only. A Pulse client log in always displays Proceed.
 - Optionally, clear the check box for **Display "Decline" Button**. If this box is not checked, the user does not have the option to decline.
 - In the **Decline Button** box, enter the text for the button that the user clicks to decline.
 - This text applies to browser-based log ins only. A Pulse client log in always displays Decline.
 - In the **Message on Decline** box, enter the text that you would like to appear when a user clicks the Decline button.
11. Click **Save Changes**.



If you enabled **Use the Sign-in Notification associated to the assigned role** you must complete the implementation by selecting the sign-in notification on the Users > User Roles > Role Name > General > UI Options page or Administrators > Admin Roles > Role Name > General > UI Options page, as applicable.

If more than one role is available to a user, the sign-in notification associated with the first role assigned is displayed.

12. Add the sign-in page in which you have customized the sign-in notification appearance to the sign-in policy.

Configuring Sign-In Pages

A sign-in page defines the customized properties in the end-user's welcome page such as the welcome text, help text, logo, header, and footer. The system allows you to create two types of sign-in pages to present to users and administrators:

Configuring Standard Sign-In Pages

Standard sign-in pages are included with the default system. You can modify standard sign-in pages. You can modify the default sign-in page that the system displays at sign-in. You can also create new standard sign-in pages that contain custom text, logo, colors, and error message text.

To create or modify a standard sign-in page:

1. Select **Authentication > Signing In > Sign-in Pages**.
2. Click **New Page**. To modify an existing page, select the link for the page you want to modify.
3. Enter a name to identify the page.
4. In the Custom text section, revise the default text used for the various screen labels. When you add text to the Instructions field, you can format text and add links using the following HTML tags: `<i>`, ``, `
`, ``, and `<ahref>`. However, the system does not rewrite links on the sign-in page (because the user has not yet been authenticated), so point only to external sites. Links to sites behind a firewall will fail.

If you use unsupported HTML tags in your custom message, the system might display the end-user's home page incorrectly.

5. (Optional) In the Header appearance section, specify a custom logo image file for the header and a different header color.
6. (Optional) In the Custom error messages section, revise the default text that is displayed to users if they encounter certificate errors.

You can include `<<host>>`, `<<port>>`, `<<protocol>>`, and `<<request>>` variables and user attribute variables, such as `<<userAttr.cn>>` in the custom error messages. These variables must be in the format `<variable>` to distinguish them from HTML tags that have the format `<tag>`.

7. (Optional) To provide custom help or additional instructions for your users, select **Show Help** button, enter a label to display on the button, and specify an HTML file to upload. Note that the system does not display images and other content referenced in this HTML page.

8. Click **Save Changes**. The changes take effect immediately, but users with active sessions might need to refresh their Web browser. Click **Restore Factory Defaults** to reset the sign-in page, user home page, and admin console appearance.

The screenshot shows the 'New Sign-In Page' configuration page. It includes the following sections and fields:

- Custom text:**
 - Welcome message:
 - Portal name:
 - Submit button:
 - Instructions:
 - Username:
 - Password:
 - Realm:
- Header appearance:**
 - Current appearance:
 - Logo image:
 - Background color:
- Custom error messages:**
 - Missing certificate:
 - Invalid certificate:
- Sign-in Notification appearance:**
 - Sign-in Notification:
 - Notification title:
 - Proceed button:
 - Decline button:
 - Message on Decline:
 - Post Auth Notification:
 - Notification title:
 - Proceed button:
 - Decline button:
 - Message on Decline:
- Show Help button:**
 - Show Help button:
 - HTML file:

A **Save Changes** button is located at the bottom left of the page.

Configuring Custom Sign-In Pages

Customized sign-in pages are HTML pages that you produce using the Template Toolkit and upload in the form of an archived ZIP file. The customized sign-in pages enable you to use your own pages rather than modify the standard sign-in pages.

To upload Custom Sign-In Pages:

1. Select **Authentication > Signing In > Sign-in Pages**.
2. Click **Sample** to download the Sample Folder as ZIP and save it on local disk.

Signing In > Sign-In Page > Custom Sign-In Pages

Custom Sign-In Pages

Custom sign-in pages allow you to provide customized templates for various pages that may appear during the sign-in process. Refer to the documentation for information about creating valid templates.

Sign-in Pages

Name:

Label to reference the custom sign-in pages.

Page Type: Access

Use Custom Page for the Pulse Desktop Client Logon
The Pulse Desktop Client will open a web browser and use custom pages for authentication instead of standard login prompts.

Prompt the secondary credentials on the second page
These labels appear when a realm using this sign-in page specifies a secondary authentication server that requires user input. These are only applicable to user sign-in pages. This option is not applicable when TOTP authentication server is selected as secondary auth-server for this realm, in which case token input from user is always taken from the second page.

Templates File: No file chosen
Zip file containing the custom templates and assets.

Current Template File:
 Size 196808 bytes. Uploaded on Tue Oct 4 11:44:53 2016

Skip validation checks during upload

Sample Templates Files
The following sample templates may be useful in producing your own customized sign-in page templates. Click to download the sample files, edit them to fit your needs, and then upload them.

This is a basic set of templates that works for most cases.

This is a set of templates for ACE Authentication.

This is an example which demonstrates how to protect against hardware keystroke loggers.

Notices:
WARNING: Page PleaseWait is out of date. It is recommended you re-customize this page from the latest sample zip file

3. Copy the following files after unzipping the folder (locally saved in previous step):

- UserAdmin-add-user.thtml
- UserAdmin-add-bulk-users.thtml
- UserAdmin-update-user.thtml
- Logout.thtml
- PleaseWait.thtml

4. Open the previously downloaded Sample Custom Sign-in folder and replace the files.
5. Select all the files and create *.ZIP file for uploading custom sign-in page.
6. Upload the new custom sign-in page and click **Save Changes**.

Using the Initial Setup Wizard

Overview

The initial setup wizard allows you to quickly configure IPS to ensure that the IPS device is configured effectively and efficiently. You can open the initial setup wizard through Wizards > Initial Setup > Configure. As a best practice, it is recommended to configure Profiling as a first step so that all the network devices are discovered. You can then launch the wizard to configure the enforcement policies on the discovered devices.

Using the initial setup wizard, you can configure IPS for the following use cases:

- Network visibility using Profiler functionality
- Layer 2 enforcement through 802.1X, MAC authentication, and SNMP for endpoints.
- Easy deployment for guest or BYOD access

Benefits

The initial setup wizard provides the following benefits:

- Provides quick onboarding of existing Pulse Connect Secure (ICS) users to IPS with a mechanism to import existing ICS policy configuration into IPS.
- Allows users to easily and quickly deploy IPS based for the desired use case (network visibility, enforcement, and guest access).

Prerequisites

You must keep the following information ready before configuring the IPS device:

- NTP server address and other details.
- The license SKU or license server details. The IPS appliance is added as a license client with necessary licenses to be leased.
- Authentication servers (AD/LDAP) must have groups defined for different roles so that corresponding access can be configured for L2 enforcement use case.

- The list of switches along with IP address and other parameters such as VLAN information for different set of users.
- Administrator account details of ICS for fetching the authentication server and role details.
- Fingerprint database, subnets to scan, and switch details for Profiling the network.

Limitations

The following are the limitations:

- Supports only layer 2 enforcement use cases.
- The initial setup wizard is supported only with the new UI.
- You can configure each use case only once using the wizard and cannot edit the configurations once it is completed.

Configuring IPS using Initial Setup Wizard

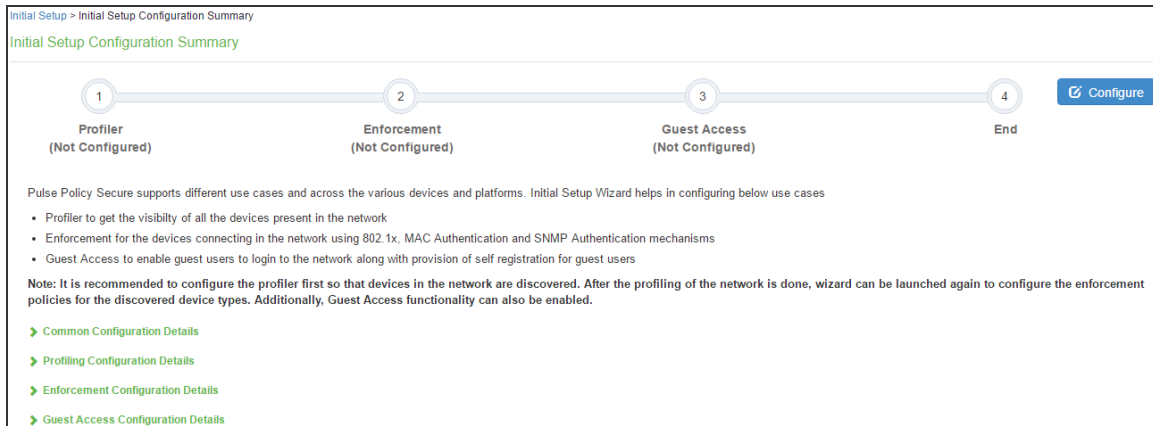
This section covers the configuration using initial setup wizard.

You can launch the initial setup wizard using:

- Select **Wizards > Initial Wizard > Configure**
- Select **Wizards > Initial Wizard > Configuration Summary**

The configuration summary page shows the configured/ not configured use cases and the corresponding details. It is recommended to configure the use cases using the configuration summary page.

The following figure shows the configuration summary page for a fresh installation.



Basic Settings

Configuring System Date and Time

The time synchronization between IPS and another component is very critical. You can easily configure the system date and time using the initial setup wizard. The system date and time can be configured manually or you can configure a network time protocol (NTP) server. It is recommended to use a public NTP server for time synchronization.

To set the system date and time:

1. Select **Wizards > Initial Setup > Configure**.
2. Select the deployment use case.
3. Select your time zone. Selecting the appropriate time zone enables the system to automatically adjust the time for Daylight Saving Time changes.
 - Use NTP Server- Enter the fully qualified domain name or IP address for the NTP server.
 - Set Time Manually- Enter the date (MM/DD/YY) and time. You can click Get from Browser to automatically populate the Date and Time.

4. Click **Set Date and Time**.

The screenshot shows the 'Initial Setup' wizard interface. On the left is a navigation menu with items: Introduction, Use Cases, System Settings (highlighted), Switch Configuration, Enforcement, Pulse Connect Secure Configuration, Authentication Servers, Roles, and Summary. The main content area is titled 'Date and Time' and contains the following elements:

- 'Select TimeZone' dropdown menu showing '(GMT-12:00) Eniwetok, Kwajalein'.
- Radio buttons for 'Use NTP Server' (selected) and 'Set Time Manually'.
- An input field for 'NTP server' containing 'NTP server'.
- A 'Get from Browser' button.
- An example timestamp: '@example: 12/28/2016 10:51:39 AM'.
- A 'Set Date & Time' button.

Below the 'Date and Time' section is the 'Licenses' section:

- 'License Keys' label above a large empty text area.
- A green arrow icon and text: 'Configure License Server'.
- An 'Install License' button with a document icon.

At the bottom of the wizard, there is a 'Cancel' button on the left, and '< Previous' and 'Next >' buttons on the right. The status bar at the very bottom shows 'localhost2 (500 users)' and '0 licenses'.

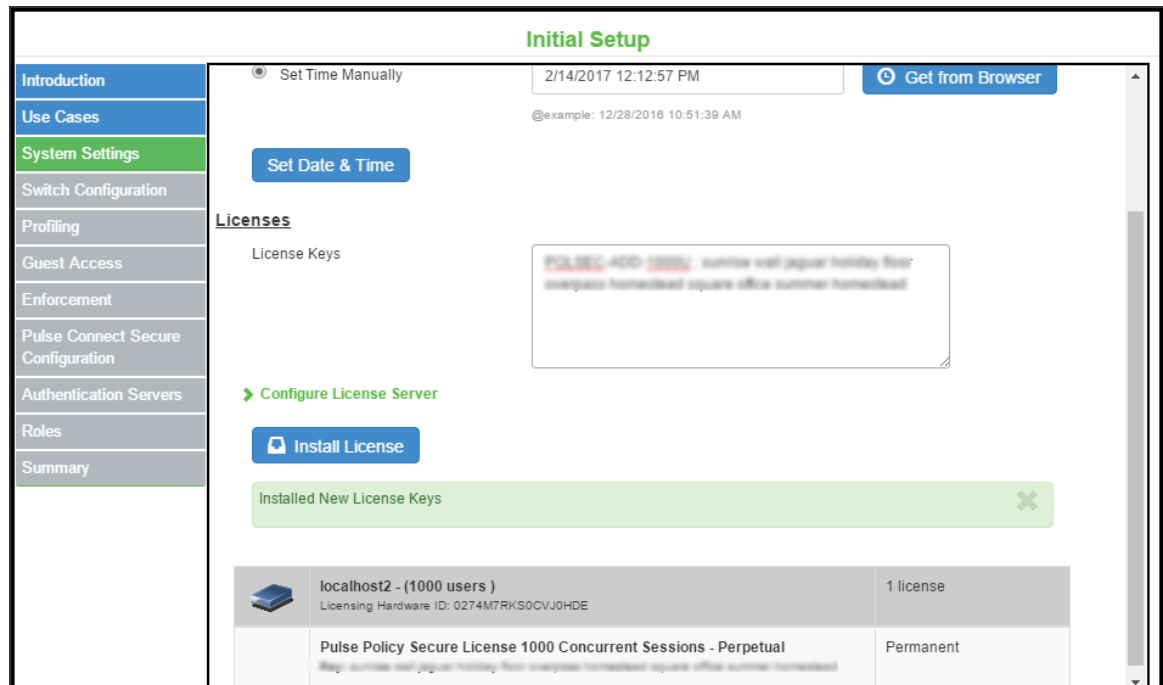
Configuring License

The license can be applied in 2 ways:

- Manually by entering the license key
- License Server

To apply the license manually:

1. Enter the license keys obtained through license key generation.
2. Click **Install License**.



To configure through the license server:

1. Enter IP address or hostname of license server.
2. Enter a unique ID for the client. This ID is used to communicate and verify the client with the license server.
3. Select the network to communicate with the license server from the Preferred Network menu. The available options are internal (default), external, and management.

- Select the **Verify SSL Certificate** check box if you want the client to verify the server's SSL certificate when establishing communication with it.

Configure License Server

Server IP/Hostname: 1.1.1.1

Lease Client ID: xxx


Password: ...

Preferred Network: internal

Verify SSL Certificate

Install License

Installed New License Keys

 localhost2 - (1000 users) Licensing Hardware ID: 0274M7RKS0CVJ0HDE	1 license
Pulse Policy Secure License 1000 Concurrent Sessions - Perpetual Key: ...	Permanent

Cancel < Previous Next >

Configuring Profiling for Network Visibility

Profiler dynamically identifies and classifies endpoints across managed and unmanaged endpoint devices, so that access to network and resources can be controlled based on the type of the device. It also helps you to get visibility so that necessary security policies for corporate access, BYOD, and guest access can be enforced.

To enable profiling on your network:

1. Select **Enable Profiling to get visibility of devices in the network**.

Initial Setup

Introduction

Use Cases

System Settings

Switch Configuration

Profiling

Summary

Use cases and Features

(Note: It is recommended to configure the profiler first so that devices in the network are discovered. After the profiling of the network is done, wizard can be launched again to configure the enforcement policies for the discovered device types.)

- Enable profiling to get visibility of devices in the network
- Enable enforcement and authentication mechanisms for the devices connecting to the network
 - Fetch configuration details from another Pulse Connect Secure server
 - Enable guest access for providing access to guest users

Prerequisite

Below are the details required for configuring PPS through this wizard

- **License Details**
License SKU or License server details are required. In case of license server, this PPS box needs to be added as a license client with necessary licenses to be leased configured
- **Profiling Details**
Fingerbank database, Subnet and Switch details for profiling the network and provide visibility
- **Switch Details**
List of switches that we want to be used for providing the access to the end users and different VLANs on the switch for different set of users.

Cancel < Previous Next >

2. Configure system date and time. See [Configuring System Date and Time](#)
3. Configure license. See [Configuring License](#)
4. You can add an SNMP device manually through Add New Switch configuration or automatically discover SNMP devices through Device Discovery.

5. To discover SNMP v2 devices:

- Select the SNMP version as v2
- Enter the IP address/range and community string.

Initial Setup

Introduction

Use Cases

System Settings

Switch Configuration

Profiling

Guest Access

Enforcement

Pulse Connect Secure Configuration

Authentication Servers

Roles



Summary

What switches do you have?



Switch can be used as an Infranet Enforcer with Pulse Policy Secure. With this solution, Pulse Policy Secure is the policy decision point, while the switch is the policy enforcement point.

▼ Discover Switches

IP Address/Range: SNMP Version:

Community String:  

► Add New Switch

Name	IP Address	SNMP	Radius Client
ruckus	10.204.88.12	v2	 

6. To discover SNMP v3 devices:

- Enter the IP address/range
- Select the SNMP version as v3
- Select the desired Authentication protocol and Privacy protocol.
- Enter the Authentication password and Privacy password.
- Click the search icon.

Initial Setup

Introduction

Use Cases

System Settings

Switch Configuration

Profiling

Guest Access

Enforcement

Pulse Connect Secure Configuration

Authentication Servers

Roles

Summary

What switches do you have?

Switch can be used as an Infranet Enforcer with Pulse Policy Secure. With this solution, Pulse Policy Secure is the policy decision point, while the switch is the policy enforcement point.

➤ Discover Switches





IP Address/Range: SNMP Version:

Username: Authentication Protocol: Authentication Password:

Privacy Protocol: Privacy Password:

🔍 ↻

➤ Add New Switch

Name	IP Address	SNMP	Radius Client
switch	10.204.88.12	v3	 
switch	10.204.88.12	v2	 

7. To add a new switch:

- Enter the name and IP address of the switch
- Select the Make/Model of the switch
- Under SNMP configuration, select the SNMP version- v2/v3
 - For SNMP v2, enter the read community string.
 - For SNMPv3, enter the authentication password, privacy password and select the authentication protocol and privacy protocol.
- Click **Save**.

The screenshot shows the 'Initial Setup' wizard interface. On the left is a navigation menu with options: Introduction, Use Cases, System Settings, Switch Configuration (highlighted), Profiling, and Summary. The main content area is titled 'What switches do you have?' and includes a description: 'Switch can be used as an Infranet Enforcer with Pulse Policy Secure. With this solution, Pulse Policy Secure is the policy decision point, while the switch is the policy enforcement point.' Below this are sections for 'Discover Switches', 'Add New Switch', and 'SNMP Configuration'. The 'Add New Switch' section contains three input fields: 'Name' (xyz), 'IP Address' (10.204.88.15), and 'Make/Model' (HP). The 'SNMP Configuration' section has 'SNMP Version' set to v2 and 'Read Community String' set to public. At the bottom of the form are 'Save' and 'Cancel' buttons. Below the form is a table listing the added switch:

Name	IP Address	SNMP	Radius Client
xyz	10.204.88.15	v2	

At the bottom of the screen are 'Cancel', '< Previous', and 'Next >' buttons.

8. Click **Next**.
9. Select **Browse** and upload the fingerprint database downloaded from the Ivanti portal.
10. Select the DHCP sniffing mode that is whether to run the DHCP sniffing on DHCP helper (Internal Port) or RSPAN (External Port).
11. Under WMI configuration, specify WMI profiler user name and password to fetch endpoint information from remote desktops running Microsoft Windows. The WMI profiler collects granular OS level information such as accurate OS version and patch level.
12. Add one or more subnets that can be included or excluded for fingerprinting devices using Nmap target scans. Nmap target scan is only performed on valid IP addresses in the subnet.

13. Enter the subnet details and Click **Add**.

Initial Setup

Introduction

Use Cases

System Settings

Switch Configuration

Profiling

Guest Access

Enforcement

Pulse Connect Secure Configuration

Authentication Servers

Roles

Summary

Profiling functionality details

Profiling is used to profile various devices on the network. Profiling is supported through DHCP finger printing, SNMP,Nmap.

Upload Fingerprint Database fpdb-22.pkg

DHCP Sniffing Mode

▼ **WMI Configuration**

Username Password

Endpoint IP

Subnet	Collector	
<input type="text" value="@Example: 192.168.1.0/24"/>	<input type="checkbox"/> Nmap <input type="checkbox"/> WMI	<input type="button" value="Add"/>
10.204.0.0/16	Nmap	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Configuring Layer 2 Enforcement

The following enforcements are supported for the devices connecting to the network.


- 802.1X
- MAC Authentication
- SNMP

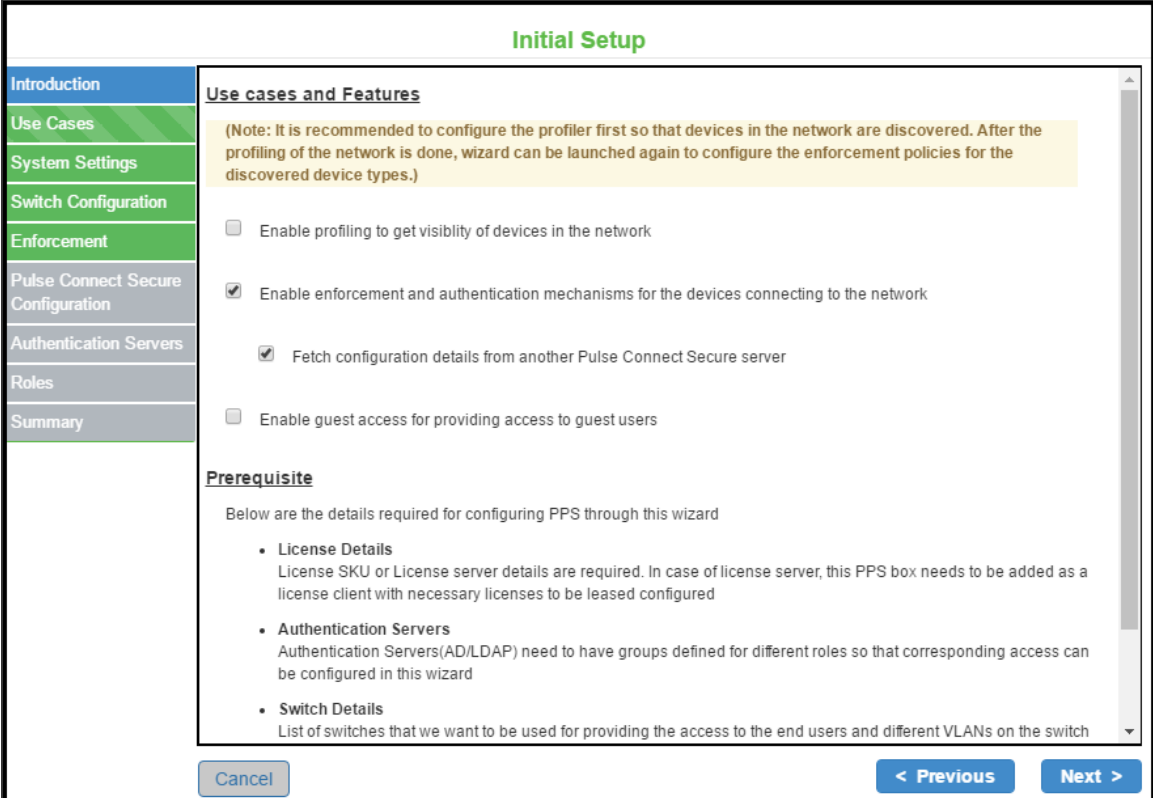
Before you begin:

As a best practice, it is recommended to configure Profiling as a first step so that all the network devices are discovered. You can then launch the wizard to configure the enforcement policies on the discovered devices.

To configure enforcement and authentication mechanism:

1. Select **Enable enforcement and authentication mechanism for the devices connecting to the network.**

 Profiling is enabled by default when you enable enforcement and authentication.



Initial Setup

Introduction

Use Cases

System Settings

Switch Configuration

Enforcement

Pulse Connect Secure Configuration

Authentication Servers

Roles

Summary

Use cases and Features

(Note: It is recommended to configure the profiler first so that devices in the network are discovered. After the profiling of the network is done, wizard can be launched again to configure the enforcement policies for the discovered device types.)

- Enable profiling to get visibility of devices in the network
- Enable enforcement and authentication mechanisms for the devices connecting to the network
- Fetch configuration details from another Pulse Connect Secure server
- Enable guest access for providing access to guest users

Prerequisite

Below are the details required for configuring PPS through this wizard

- License Details**
License SKU or License server details are required. In case of license server, this PPS box needs to be added as a license client with necessary licenses to be leased configured
- Authentication Servers**
Authentication Servers(AD/LDAP) need to have groups defined for different roles so that corresponding access can be configured in this wizard
- Switch Details**
List of switches that we want to be used for providing the access to the end users and different VLANs on the switch

2. Configure basic settings. See Basic Settings.

3. Configure the switch. Complete the configurations as described in the following table.

Discover Switches	
SNMP v2	<ul style="list-style-type: none"> • Enter the IP address/range and community string. • Enter the IP address/range
SNMP v3	<ul style="list-style-type: none"> • Select the desired Authentication protocol and Privacy protocol. • Enter the Authentication password and Privacy password. • Click the search icon.
Add New Switch	
Name	Enter a name to label the RADIUS client. You can assign any name to a RADIUS client entry, use the device's SSID or IPv4/IPv6 address to avoid confusion.
IP Address	Enter the IPv4/IPv6 address of the switch.
Make/Model	Select the make/model of the switch vendor. The make/model selection tells IPS which dictionary of RADIUS attributes to use when communicating with this client.
RADIUS Client Configuration	
IP Address Range	Enter the number of IP addresses in the IP address range for the switch/WLC, starting with the address you specified for IP Address. You can specify a range up to a maximum of 32,768 addresses.
Shared Secret	Enter the RADIUS shared secret. A RADIUS shared secret is a case-sensitive password used to validate communications between IPS and switch.
SNMP Configuration	

Discover Switches	
SNMP Version	<ul style="list-style-type: none"> • Select the SNMP version (v2/v3). • For SNMP v2, enter the read community string. • For SNMPv3, enter the authentication password, privacy password and select the authentication protocol and privacy protocol. • Select Use for enforcement to use the SNMP device for SNMP enforcement.

Initial Setup

- Introduction
- Use Cases
- System Settings
- Switch Configuration
- Profiling
- Enforcement
- Pulse Connect Secure Configuration
- Authentication Servers
- Roles
- Summary

▼ Add New Switch

Name	IP Address	Make/Model
<input type="text" value="xyz"/>	<input type="text" value="10.204.88.15"/>	<input type="text" value="HP"/>

▼ Radius Client Configuration

IP Address Range	Shared Secret
<input type="text" value="1"/>	<input type="text"/>

▼ SNMP Configuration

SNMP Version	Write/Trap User Same? <input checked="" type="checkbox"/>	Use for Enforcement <input checked="" type="checkbox"/>
<input type="text" value="v2"/>		
Read Community String		
<input type="text" value="public"/>		

Name	IP Address	SNMP	Radius Client
xyz	10.204.88.15	v2	

Initial Setup

- Introduction
- Use Cases
- System Settings
- Switch Configuration
- Profiling
- Enforcement
- Pulse Connect Secure Configuration
- Authentication Servers
- Roles
- Summary

▼ Add New Switch

Name <input type="text" value="xyz"/>	IP Address <input type="text" value="10.204.88.15"/>	Make/Model <input type="text" value="HP"/>
--	---	---

▼ Radius Client Configuration

IP Address Range <input type="text" value="1"/>	Shared Secret <input type="text"/>
--	---------------------------------------


▼ SNMP Configuration

SNMP Version <input type="text" value="v3"/>	Write/Trap User Same? <input checked="" type="checkbox"/>	Use for Enforcement <input checked="" type="checkbox"/>
---	---	---

Read User Credentials

Username <input type="text"/>	Authentication Protocol <input type="text" value="MD5"/>	Authentication Password <input type="text"/>
Privacy Protocol <input type="text" value="None"/>	Privacy Password <input type="text"/>	

4. Configure the enforcement for devices, which includes laptops, smart phones, VOIP phones, and unmanaged devices.

 If profiling is enabled the device platform types are automatically enabled.

Device Type	Platforms	Authentication Type	Additional Support
Laptops	<ul style="list-style-type: none">• Windows• MAC• Linux	<ul style="list-style-type: none">• 802.1X• SNMP	Host Checker
Smart phones	<ul style="list-style-type: none">• Android• iOS	802.1X	NA
VOIP phones	NA	<ul style="list-style-type: none">• 802.1X• MAC	NA
Unmanaged devices	NA	MAC	NA

5. Enter the SSID for 802.1X. Use comma as a delimiter for entering multiple SSID's.

Initial Setup

Introduction

Use Cases

System Settings

Switch Configuration

Profiling

Guest Access

Enforcement

Pulse Connect Secure Configuration

Authentication Servers

Roles

Summary

What kind of enforcement do you want to support?

Laptops

Windows Macintosh Linux

Enable compliance check ON OFF

Select Authentication types 802.1x SNMP

Smart Phones

Android iOS

Note: Only 802.1x authentication supported

VOIP Phones

802.1x MAC

Select Authentication type

Unmanaged Devices

Printers

Note: Only MAC authentication supported

SSIDs for 802.1x

Note: Multiple SSIDs should be comma separated

Importing Configurations from Pulse Connect Secure

Importing Configurations from Pulse Connect Secure

The existing configurations in ICS can be imported to IPS for quickly configuring the IPS device.

The following configurations can be imported from ICS:

- Authentication servers
- Role names
- Host Checker compliance policies

To import the ICS device configurations to IPS device:

1. Select **Fetch configuration details from another Pulse Connect Secure server**.
2. Enter the ICS sign-in URL.
3. Enter the admin username.

4. Enter the password
5. Enter the realm information.
6. Click **Fetch**. The list of imported authentication servers, roles, and Host Checker compliance policies are displayed.



If you try to import the configuration multiple times. The configurations will be overwritten with the newer configuration.

Initial Setup

Successfully fetched configuration details from Pulse Connect Secure

This will import configuration from existing Pulse Connect Secure instance and use them in configuring Pulse Policy Secure. Below are the list of configuration items that will be fetched from Pulse Connect Secure.

- Authentication servers
- Roles

Admin SignIn URL

Username

Password

Admin Realm

Fetch

Note: Empty policies and thirdparty policies will not be imported.

List of imported Authentication Servers

Idap

List of imported Roles

AAA-Role

List of imported Host Checker Compliance Policies

PS-Check

Cancel
< Previous
Next >

Authentication Server

Authentication server is used for authentication and verifying group membership. It validates the user credentials and then provides the required access. It also maps users to roles based on either Light Weight Directory Access protocol (LDAP) or Active Directory (AD) group information. The initial setup wizard supports AD and LDAP authentication servers for user authentication. LDAP is supported for device authentication based on MAC address.

To add the authentication server:

1. Select the **Server Type** (AD/LDAP).

Initial Setup

- Introduction
- Use Cases
- System Settings
- Switch Configuration
- Profiling
- Guest Access
- Enforcement
- Pulse Connect Secure Configuration
- Authentication Servers**
- Roles
- Compliance Check
- Summary

What Authentication Servers do you have?





Authentication Servers are used for authenticating the end users logging onto the network. Select appropriate servers for authentication.

User Authentication:
This server will be used for authenticating end users

MAC Authentication:
This server will be used for authenticating devices using MAC Address
Note: Only LDAP servers can be used

List of available Servers

Add Server Type:

AuthServer Name	AuthServer Type	Domain/HostName	
ldap	LDAP	10.209.114.249:389	 
AD	ACTIVE_DIRECTORY	pcsqalab	 

- For Active Directory, enter the server name, user credentials, Kerberos realm, and domain. You can click Test to verify the configuration.

The screenshot shows the 'Initial Setup' wizard with the 'Authentication Servers' section selected in the left-hand navigation menu. The main content area is titled 'What Authentication Servers do you have?' and contains the following configuration options:

- User Authentication:** A dropdown menu set to 'AD'. Below it, a note states: 'This server will be used for authenticating end users.'
- MAC Authentication:** A dropdown menu set to 'ldap'. Below it, a note states: 'This server will be used for authenticating devices using MAC Address. Note: Only LDAP servers can be used.'
- List of available Servers:** A dropdown menu set to 'Active Directory'.
- Active Directory Configuration:**
 - Server Name:** A text input field containing 'AD'.
 - Username:** A text input field containing 'administrator'.
 - Password:** A text input field containing '*****'.
 - Kerberos Realm:** A text input field containing 'pcsqalab.net'.
 - Domain:** A text input field containing 'pcsqalab'.

At the bottom of the configuration area, there are three buttons: 'Test', 'Save', and 'Reset'. Below these buttons is a table with the following headers: 'AuthServer Name', 'AuthServer Type', and 'Domain/HostName'. The table is currently empty. At the bottom of the wizard, there are three navigation buttons: 'Cancel', '< Previous', and 'Next >'.

- For LDAP, enter the server name, LDAP server type (Generic, AD, iPlanet, Novell eDirectory, Profiler), connection type, filter, admin DN, base DN, unique variable for filtering, group member attribute, and group base DN.

Initial Setup

Introduction
Use Cases
System Settings
Switch Configuration
Profiling
Guest Access
Enforcement
Pulse Connect Secure Configuration
Authentication Servers
Roles
Compliance Check
Summary

User Authentication: AD
This server will be used for authenticating end users

MAC Authentication: ldap
This server will be used for authenticating devices using MAC Address
 Note: Only LDAP servers can be used

List of available Servers

Add Server Type: LDAP

LDAP Server	Host	Server Type
ldap	10.204.90.216	Active Directory

Port: 389
 Connection Type: Unencrypted
 Filter: macAddress=<USER>

Admin DN: cn=Administrator,cn=users,dc=u
 Password: *****
 Base DN: OU=MACAddresses,OU=MAC,d

Group Filter: (&(objectClass=group)(cn=*))
 Group Member Attribute: member
 Group BaseDN: OU=MACGroups,OU=MAC,dc=u

Cancel < Previous Next >

- Configure the required authentication server for user authentication and machine authentication.

Roles


A user role defines user session parameters (session settings and options) and personalization settings (user interface customization).



You can reuse the roles imported from ICS and then configure the VLAN and group information.

To add a role name:

1. Enter the role name and VLAN information.
2. Select the **AD group or LDAP group**.

 If the AD or LDAP group information is not available you must add the group information manually.

3. Click **Add (+)** icon.
4. Enter the remediation role and the VLAN information.
5. Enter the role name and the VLAN information for unmanaged devices.

Initial Setup

Introduction

Use Cases

System Settings

Switch Configuration

Profiling

Guest Access

Enforcement

Pulse Connect Secure Configuration

Authentication Servers

Roles

Compliance Check

Summary

What Roles do you have?

User Roles defines user session parameters(session settings and options) and personalisation settings(User Interface customization)


Role Name	VLAN	AD Group	LDAP Group	
<input type="text" value="Enter Name"/>	<input type="text" value="VLAN"/>	<input type="text" value="- Choose User Group"/>	<input type="text" value="- Choose User Group"/>	+
Role	65	domain users	cameras	✎ 🗑

Remediation Role

Unmanaged Devices Role

Compliance Check

IPS offers a variety of endpoint host checks to ensure compliance, including predefined checks for third-party endpoint security software including anti-virus, firewall, anti-malware/anti-spyware applications.

 You can reuse the compliance policies from ICS.

To configure IPS for endpoint compliance:

1. Enter the rule name.
2. Select the platform type- Windows, Linux, MAC.
3. Select the rule type.



Antivirus, Firewall, and Process policies are supported for Windows and MAC platforms. Process policy is supported for Linux platform.

4. To enable remediation action, select **Enable Remediation Action**.
5. Click + **Add**.

Initial Setup

Introduction

Use Cases

System Settings

Switch Configuration

Profiling

Guest Access

Enforcement

Pulse Connect Secure Configuration

Authentication Servers

Roles

Compliance Check

Summary

▼ Add HostChecker Policy

RuleName Platform - Select Platform Type -

Type - Select Compliance Type -

Enable Remediation Action
+ Add
Reset

InitialSetupHCPolicy				
Rule Name	Platform	Compliance Type	Remediation	
RuleName	windows	Firewall	✓	✎ 🗑️

Policy Name	Windows	Mac	Linux	Enforce
PS-Check	Process ✓	Process ✓	Process ✓	☑️
InitialSetup_HostCheckerPolicy	Firewall ✓			☐

Note: Compliance policies selected will be applied based on the platform and the rules configured for the hostchecker policy.

Cancel
< Previous
Next >

Configuring Guest Authentication

Guest access feature on IPS enables guest users to access the network through a self-registration process. The guest users self-register for network access from their device. Upon successful registration, the guest users are notified with the user credentials and other details through SMS or email.

To configure guest authentication:

1. Select **Wizards > Initial Setup > Configuration Summary**.
2. Select **Enable guest access for providing access to guest users**.

The screenshot shows the 'Initial Setup' wizard at the 'Configuration Summary' step. The left sidebar contains a navigation menu with the following items: Introduction, Use Cases, System Settings, Switch Configuration, Guest Access (highlighted in green), Compliance Check, and Summary. The main content area is titled 'Use cases and Features' and contains the following text and options:

Use cases and Features

(Note: It is recommended to configure the profiler first so that devices in the network are discovered. After the profiling of the network is done, wizard can be launched again to configure the enforcement policies for the discovered device types.)

- Enable profiling to get visibility of devices in the network
- Enable enforcement and authentication mechanisms for the devices connecting to the network
- Fetch configuration details from another Pulse Connect Secure server
- Enable guest access for providing access to guest users

Prerequisite

Below are the details required for configuring PPS through this wizard

- **License Details**
License SKU or License server details are required. In case of license server, this PPS box needs to be added as a license client with necessary licenses to be leased configured
- **Switch Details**
List of switches that we want to be used for providing the access to the end users and different VLANs on the switch for different set of users.
Note: VLANs on all the switches need to be configured similarly
- **Guest Authentication**

At the bottom of the screen, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

- Enter the VLAN information for the guest user.

- (Optional) Select **Create Guest Administrator Account** and enter the username and password.
- (Optional) Select **Enable Self Registration**.
The SMTP and SMS configuration settings must be configured to enable guest users to create user accounts on their own.
- (Optional) Select **Send Email to Guest Users** and then enter the IP address or host name of the SMTP server, email address, and log in credentials of the SMTP server.
- (Optional) Select **Send SMS to Guest Users** and then select the SMS gateway type, gateway URL, SMS gateway log in credentials, API ID, and the mobile number of the guest user.
- Configure the switch as described in table.

Add New Switch	
Name	Enter a name to label the RADIUS client. You can assign any name to a RADIUS client entry, use the device's SSID or IPv4/IPv6 address to avoid confusion.

Add New Switch	
IP Address	Enter the IPv4/IPv6 address of the switch.
Make/Model	Select the make/model of the switch vendor. The make/model selection tells IPS which dictionary of RADIUS attributes to use when communicating with this client.
RADIUS Client Configuration	
IP Address Range	Enter the number of IP addresses in the IP address range for the switch/WLC, starting with the address you specified for IP Address. You can specify a range up to a maximum of 32,768 addresses.
Shared Secret	Enter the RADIUS shared secret. A RADIUS shared secret is a case-sensitive password used to validate communications between IPS and switch.

Initial Setup

Introduction

Use Cases

System Settings

Switch Configuration

Guest Access

Compliance Check

Summary

What switches do you have?

Switch can be used as an Infranet Enforcer with Pulse Policy Secure. With this solution, Pulse Policy Secure is the policy decision point, while the switch is the policy enforcement point.

▼ Add New Switch

Name	IP Address	Make/Model
<input type="text" value="10.204.88.12"/>	<input type="text" value="10.204.88.12"/>	<input type="text" value="Ruckus Wireless"/>

▼ Radius Client Configuration

IP Address Range	Shared Secret	Ruckus Password
<input type="text" value="1"/>	<input type="text" value="*****"/>	<input type="text"/>

Validate Ruckus Server Certificate

Save
Cancel

Name	IP Address	SNMP	Radius Client
10.204.88.12	10.204.88.12	None	✓

Cancel
< Previous
Next >

Verification and Troubleshooting

You can verify the configuration summary page for any errors during the initial setup configuration and perform the troubleshooting task based on the issue. The wizard captures the summary of the configurations before proceeding with enabling the corresponding use case on IPS. If needed you can modify the required configurations before completing the configuration.

The screenshot shows the 'Initial Setup' wizard's summary page. On the left is a navigation menu with options: Introduction, Use Cases, System Settings, Switch Configuration, Profiling, Guest Access, Enforcement, Pulse Connect Secure Configuration, Authentication Servers, Roles, Compliance Check, and Summary (highlighted in green). The main content area is titled 'What is getting configured?' and lists the following details:

- Usecases Selected:** Profiling, Guest Access, Enforcement
- Switch Settings:** ProCurve Switch 2810-24G(HP)
- Profiler Settings:** Subnets:
- Guest Access Settings:** Guest VLAN: 65
- Enforcement:**
 - Windows - Compliance: ON Authentication: 802.1x, SNMP
 - Mac - Compliance: ON Authentication: 802.1x, SNMP
 - Linux - Compliance: ON Authentication: 802.1x, SNMP
 - Android - Authentication: 802.1x
 - IOS - Authentication: 802.1x
 - VOIP - Authentication: 802.1x, MAC
 - Unmanaged Devices - Authentication: MAC
- Authentication Servers:**
 - User Authentication Server: AD(ACTIVE DIRECTORY)
 - MAC Authentication Server: LDAP(LDAP)
- Roles Configured:**
 - Role(65)
 - Remediation Role: Rem-Role(74)
 - Role For Unmanaged devices: Unmanaged-Roles(60)
- Compliance Settings:** InitialSetup_HostCheckerPolicy:

At the bottom, there are three buttons: 'Cancel', '< Previous', and 'Finish >'.

The following figure shows the final configuration summary page. You can verify the common configuration, profiling, enforcement, guest access configuration details.

The screenshot shows the 'Initial Setup Configuration Summary' page. At the top, it says 'Initial Setup > Initial Setup Configuration Summary'. Below this is a progress bar with four steps: 'Profiler (Completed)', 'Enforcement (Completed)', 'Guest Access (Completed)', and 'End'. A 'Configure' button is visible at the end of the progress bar. Below the progress bar, there is a note: 'Pulse Policy Secure supports different use cases and across the various devices and platforms. Initial Setup Wizard helps in configuring below use cases' followed by a bulleted list:

- Profiler to get the visibility of all the devices present in the network
- Enforcement for the devices connecting in the network using 802.1x, MAC Authentication and SNMP Authentication mechanisms
- Guest Access to enable guest users to login to the network along with provision of self registration for guest users

A note follows: 'Note: It is recommended to configure the profiler first so that devices in the network are discovered. After the profiling of the network is done, wizard can be launched again to configure the enforcement policies for the discovered device types. Additionally, Guest Access functionality can also be enabled.' Below the note are four expandable sections: 'Common Configuration Details', 'Profiling Configuration Details', 'Enforcement Configuration Details', and 'Guest Access Configuration Details'.

IPS Migration Wizard

IPS Migration wizard enables seamless migration of RADIUS and TACACS+ configuration, and also automatically creates basic IPS configuration needed for these use cases to work right after migration is complete.

Prerequisites

Before proceeding with the IPS Migration wizard, export the RADIUS/TACACS+ clients' details in the form of CSV file from Cisco ACS.

Follow the below steps to export the RADIUS/TACACS+ clients' details:

1. Log in to Cisco ACS GUI.
2. Navigate to **Network Resources > Network Devices and AAA Clients**.
3. Select all the clients.
4. Click **Export**.

The screenshot shows the Cisco Secure ACS GUI interface. The main content area is titled "Network Resources > Network Devices and AAA Clients". Below this, there is a "Network Devices" section with a filter and match options. A table lists the following devices:

Name	IP Address	Description	NDG Location	NDG Device Type
Arista3500	10.204.66.33/32		All Locations:Singapore	All Device Types
Cisco2900	10.204.57.62/32, 3.4.5.1/24		All Locations:India Bangalore	All Device Types: CiscoSwitches
Cisco3560	1.2.2.2/32	Cisco 3560 LAB	All Locations:India	All Device Types: CiscoSwitches
Cisco3650-VLAN-10	1.2.2.5/32	Cisco 3560 LAB	All Locations:SFO-FIR-1:BAY-1	All Device Types: CiscoSwitches: Cisco2960
hp_client1	10.204.88.30/32		All Locations:India	All Device Types

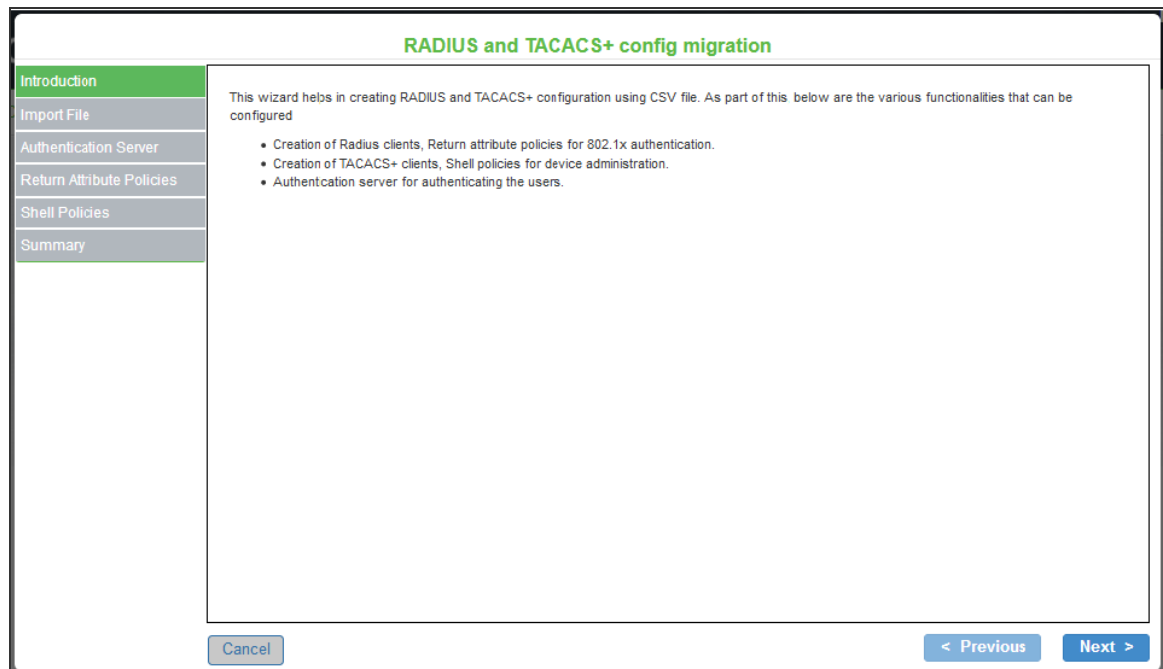
At the bottom of the table, there are buttons for "Create", "Duplicate", "Edit", "Delete", "File Operations", and "Export". The "Export" button is highlighted in the screenshot.

Configuring RADIUS and TACACS+ Migration using IPS Migration Wizard

The IPS Migration wizard helps administrators in creating RADIUS and TACACS+ configuration using the CSV file exported from Cisco ACS.

To configure RADIUS and TACACS+ migration using IPS Wizard:

1. Log in to the IPS Admin console.
2. Select **Wizards > Migration > RADIUS and TACACS+ config migration**. The Introduction window lists the configuration steps.
3. Click **Next**.



4. In the Import File window, choose the use cases for configuration import – the **RADIUS clients** check box or **TACACS+ clients** check box or both. Based on these selections, migration wizard provides steps to create the Radius policies followed by the Shell policies.
5. Click **Browse** and select the CSV file that is exported from Cisco ACS.

- Click **Next**. After receiving confirmation for successful upload, click **Next**.

RADIUS and TACACS+ config migration

Introduction

Import File

Authentication Server

Return Attribute Policies

Shell Policies


Summary

Successfully validated file chosen. Click on "Next" to continue with the configuration.

RADIUS clients

TACACS+ clients

Upload File (csv) export-net-type.csv

 At any stage of the migration wizard, you can click **Previous** to go back to the previous window or click **Cancel** to cancel the migration.

- Next step is to configure the Active Directory server. You can select one from the existing list of AD servers or add a new AD server.
 - To select from the existing list, click **Select existing server** and choose the required AD server from the list.
 - To add a new AD server, click **Add new AD server**. Enter the name, domain name, Kerberos realm, user name, password that matches with the ACS configurations.
- Click **Test** to validate the Active Directory configuration. This will take a few seconds to complete.

9. Once the validation is successful, click **Next**.

RADIUS and TACACS+ config migration

Return Attribute:

Return Attribute	Value	Action
Filter-Id		+
Filter-Id	compliant.in	🗑️

Add Session-Timeout attribute

Terminate the session Re-authenticate the session

Interface: Automatic

Available AD groups:

- domain computers
- domain controllers
- schema admins
- enterprise admins
- cert publishers
- domain admins

Selected AD groups:

- (all)

Buttons: Save Changes, Cancel, < Previous, Next >

10. In the RADIUS Return Attribute Policies window, click **New Policy** and enter a name to the Radius policy.
11. Select Location Groups.



IPS supports single location group; nested location groups are not supported. The subgroups created on ACS have to be configured as individual groups in IPS.

12. Select the **Return Attribute** check box. Select appropriate Vendor Specific Attribute as Return Attribute. In the **Value** field, define the ACL/Firewall Filter. For example, Return Attribute is **Filter-Id** and Value is compliant.in.
13. Click **Save Changes** to save the configuration.

14. Click **Next**.

RADIUS and TACACS+ config migration

- Introduction
- Import File
- Authentication Server
- Return Attribute Policies
- Shell Policies
- Summary

RADIUS Return Attribute Policies

A RADIUS return attributes policy specifies the return list attributes to send to an 802.1X network access device, such as which VLAN endpoints must use to access the network. If no policy applies, Open Port is the default action.

Policy Name:

Available Location Groups:

All Locations_India

All Locations_SFO_FIR-1_BAY-1

All Locations_Singapore

Add ->

Remove

Selected Location Groups:

All Locations_India_Bangalore

Provide full Access (Open Port)

Control the Access

VLAN:

Return Attribute:

Return Attribute	Value	Action
<input style="width: 80%;" type="text" value="Filter-Id"/>	<input style="width: 80%;" type="text"/>	+

Cancel

< Previous
Next >

RADIUS and TACACS+ config migration

Return Attribute Policies

Return Attribute:

Return Attribute	Value	Action
Filter-Id		+
Filter-Id	compliant.in	🗑️

Add Session-Timeout attribute

Terminate the session Re-authenticate the session

Interface: Automatic

Available AD groups:

- domain computers
- domain controllers
- schema admins
- enterprise admins
- cert publishers
- domain admins

Add -> Remove

Selected AD groups:

- (all)

Save Changes Cancel

Cancel < Previous Next >

15. In the Shell Policies window, click **New Policy** and enter a name to the Shell policy.
16. Define external group, device type, shell profile and the command set.
17. Click Save Changes to save the configuration.

18. Click **Next**.

RADIUS and TACACS+ config migration

- Introduction
- Import File
- Authentication Server
- Return Attribute Policies
- Shell Policies
- Summary

Shell Policies

A Shell policy specifies the privilege level, command sets/custom attributes to be sent in Authorization request to switch.

Shell Policy Name:

Available Device Groups:

All Device Types

All Device Types_CiscoSwitches_Cisco2960

Add ->

Remove

Selected Device Groups:

All Device Types_CiscoSwitches

Default Privilege:

Maximum Privilege:

Command Sets:

Command	Arguments	Action	
<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text" value="permit"/>	+

RADIUS and TACACS+ config migration

+

Please specify the action to be taken on any command that does not match any of the rule in the table above

Deny
 Permit

Custom Attributes:

Attribute	Value	Requirement	Action
<input type="text"/>	<input type="text"/>	<input type="text" value="Mandatory"/>	+

Available AD groups:

domain computers
 schema admins
 cert publishers
 domain admins
 domain users
 domain guests

Selected AD groups:

domain controllers
 enterprise admins

19. In the Summary window, verify the details and click **Finish** to complete the RADIUS and TACACS+ configuration migration.

Summary	
Signin url	migration_url
User Realm	migration_realm
Admin Realm	migration_admin_realm
Authentication server	AD Server
Location Groups	▼Location Groups List All Locations_India_Bangalore, All Locations_India, All Locations_SFO_FIR-1_BAY-1, All Locations_Singapore
RADIUS Clients	▼RADIUS Clients List Cisco2900, Cisco3560, Cisco3650-VLAN-10, hp_client1, Cisco 2960X
TACACS+ Clients	▼TACACS+ Clients List Arista3500, Cisco2900, Cisco3560, Cisco3650-VLAN-10, Cisco 2960X
RADIUS Return Attribute Policies	▼Policies List Radius policy
Device Groups	▼Device Groups List All Device Types, All Device Types_CiscoSwitches, All Device Types_CiscoSwitches_Cisco2960
Shell Policies	▼Policies List Shell policy

- Successfully created auth server with name: AD Server
- Successfully created 2 roles
- Successfully created user realm : migration_realm
- Successfully created 2 role mapping rule(s)
- Successfully created signin url :*/migration_url
- Successfully created 4 Location groups
- Successfully created 4 Radius clients
- Failed to create 1 Radius clients
- Successfully created 1 return attribute policies
- Successfully created 2 roles
- Successfully created admin realm : migration_admin_realm
- Successfully created 2 role mapping rule(s)
- Successfully created 3 Device groups
- Successfully created 5 TACACS clients
- Successfully created 1 Shell policies

For more information on 802.1X authentication and troubleshooting, see 802.1X Authentication with Cisco Switch cook book

Layer 2 Enforcement

Layer 2 enforcement means controlling network access at the point where the user attaches to the network. In a wired network, this control is at the switch port; in a wireless network the control is at the wireless access point. The network access control is accomplished through 802.1X authentication protocol (implemented on the switch or wireless AP) in conjunction with RADIUS return attributes to control switch or AP operation such as VLAN assignment and filtering.

Using the 802.1X standard we can create a strong network perimeter defense through strong admission controls that do not allow users onto the network unless they are compliant with specified policy.

Policy Enforcement using 802.1X

Overview

802.1X is an IEEE standard for port-based network access control. It provides an authentication mechanism for devices and users attempting to connect to wired and wireless LANs so that only authorized connections are allowed.

The basic components of 802.1X are:

- **Endpoints**- The endpoint is the device being authenticated. The supplicant is an agent running on the endpoint. For example, Pulse client, native supplicant, and non-Pulse Secure supplicant.
- **Authenticator/Switch**-The authenticator is a network device a managed switch or wireless access point that facilitates authentication by relaying credentials between the supplicant and authentication server.
- **Authentication Server**- IPS acts as an authentication server (typically a RADIUS server) and validates the credentials of the supplicant requesting access.

The 802.1X standard specifies the Extensible Authentication Protocol (EAP) as its encrypted message format for transmission between supplicant and authenticator.

Benefits of 802.1X Authentication

Following are the benefits of 802.1X authentication:

- Supports dynamic authentication policy using 802.1X, RADIUS, and RADIUS proxy.
- Supports RADIUS Change of Authorization (CoA) and RADIUS Disconnect, which allows devices to change the VLAN/ACL for the endpoint based on roles.
- Supports hybrid NAC deployment (802.1X for wireless network and SNMP for wired network).
- Supports backend third-party RADIUS servers through RADIUS proxy.
- Supports native client, pulse client, and third party supplicants.

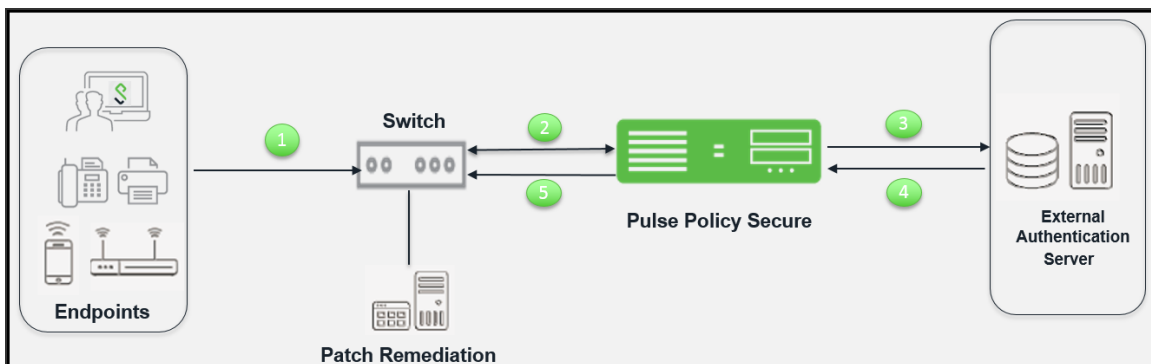
Deployments using 802.1X Authentication

The 802.1X provides authenticated access to LAN, which applies to both wireless and wired networks. In a wireless network, the 802.1X authentication occurs after the client has associated to an access point using an 802.11 association method. The wired networks use the 802.1X standard without any 802.11 association by connecting to a port on an 802.1X enabled switch.

Using 802.1X, the user is authenticated to the network by means of user credentials, such as a password, certificate, or a token card. The keys used for data encryption are generated dynamically. The authentication is not performed by the switch, but rather by IPS as the RADIUS server. The 802.1X method uses EAP messages to perform authentication. The newer EAP protocols can dynamically generate the Wired Equivalent Privacy (WEP), Temporary Key Integrity Protocol (TKIP), or Advanced Encryption Standard (AES) keys that encrypt data between the client and the wireless access point. Dynamically created keys are more difficult to break than preconfigured keys because their lifetime is much shorter. The known cryptographic attacks against WEP can be prevented by reducing the length of time that an encryption key remains in use. The encryption keys generated using EAP protocols are generated on a per-user and per-session basis. The keys are not shared among users, as they must be with preconfigured keys or preshared passphrases.

Deployment of IPS with External Authentication Server

It is difficult or impossible to maintain a centralized database of users in environments with many distributed users. You can easily pair IPS with an organization's other identity databases, such as LDAP and Active Directory to leverage existing credentials. IPS RADIUS server can forward authentication requests from a network access device (NAD) to an external Authentication server.



The authentication process is described below:

1. The endpoint connects to an 802.1X enabled switch/WLC. The endpoint exchange EAP messages using 802.1X, which contain information about user credentials and the health of the endpoint.
2. The switch receives the request and starts the RADIUS authentication with IPS.
3. IPS receives the request and then converts the request to the required format for the external authentication server.
4. If IPS successfully authenticates the user, it sends a message to the switch/WLC to allow the endpoint access to the network. The type of access granted depends on the user's identity and the health of the endpoint. For example, if the endpoint meets the requirements of all Host Checker policies, the user can have full network access. If the endpoint does not meet some security requirements, the user can be granted access to a remediation server. If the endpoint is using Pulse Client as its 802.1X supplicant, IPS and the endpoint exchange messages as necessary throughout a session (for example, to monitor the endpoint's security compliance). If the endpoint is using a native supplicant, Host Checker is not supported.
5. If the endpoint is using Pulse Client, and the endpoint meets the requirements of all Host Checker policies then IPS allows user to access the protected resources.

The user's identity and the endpoint health assessment are used to determine which VLAN to use for the switch port that the endpoint is connected to. Typically, if the endpoint does not meet minimum criteria for health assessment as defined by the administrator, the endpoint will be placed on a restricted VLAN which allows access to servers which can aid in remediating the endpoint.

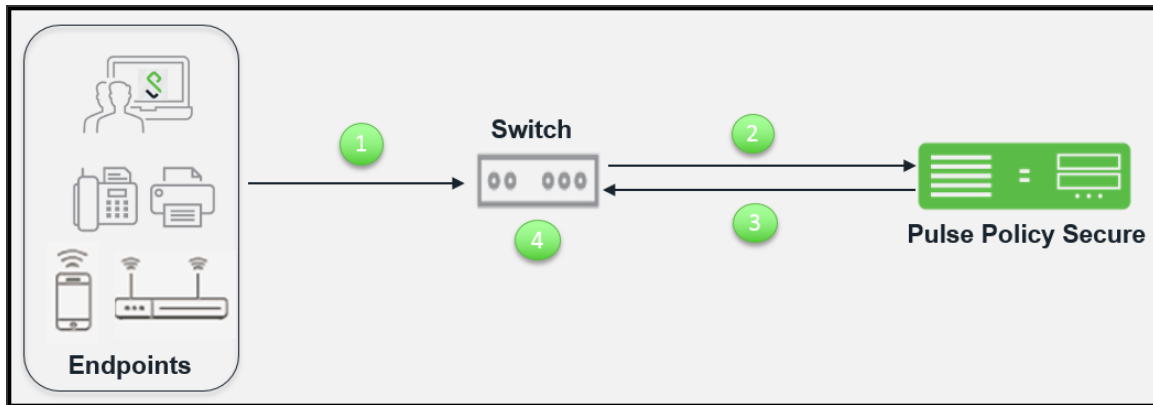
You define VLAN policies for endpoints that access switches using 802.1X. After an authenticated endpoint, has been mapped to a set of roles, the VLAN policies are evaluated and the VLAN information is communicated to the switch through RADIUS attributes. RADIUS attributes vary by make and model of switch. You specify the make and model when configuring a RADIUS client on IPS.

In addition to authenticating endpoints with 802.1X IPS RADIUS server can be used to authenticate 802.1X IP phones, switches.

Deployment of IPS as a RADIUS Server

IPS provides the RADIUS server functionality for layer 2 enforcement. Using the IPS internal RADIUS server, you can provision 802.1X authentication for endpoints. Layer 2 authentication and enforcement is used to control network access policies at the edge of the network using an 802.1X enabled switch or access point.

A RADIUS license allows you to use the IPS series device as a RADIUS appliance. To apply your initial license or to upgrade your license, select System > Configuration > Licensing in the left navigation pane.



The authentication process is described below:

1. The endpoints connect to switch over 802.1X using EAP protocol.
2. The switch receives the request and starts the RADIUS authentication with IPS.
3. IPS integrated RADIUS server receives the request and performs the authentication and then returns the attributes for controlling user access.
4. The switch uses the returned attributes to control the user access privileges on the port or service set identifier (SSID).

The following RADIUS configuration options are available only with RADIUS license.

- Host Checker Custom: Statement of Health policy- When you apply both a RADIUS license and an MS-NAP license, you can configure an Endpoint Security policy by way of the Host Checker policy. If you have only a RADIUS license, the Endpoint Security menu is not available.
- RADIUS User Count- This feature allows you to create RADIUS users. To view the number of RADIUS users, select System > Status. The number of RADIUS users does not count against the concurrent user license if you have both a RADIUS license and a user license installed.

The following features are not available with RADIUS only license:

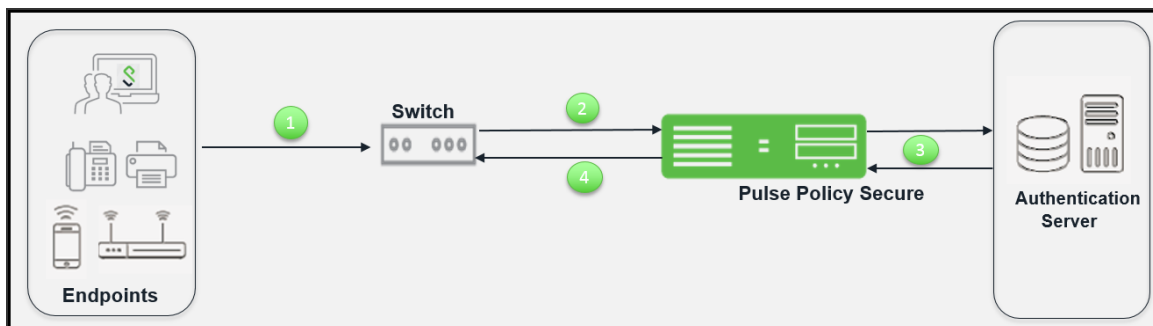
- IF-MAP Federation
- Infranet Enforcer

- Host Enforcer
- Endpoint Security
- Push Configuration
- SiteMinder and MDM Authentication servers
- Sign-in Notifications
- Sensors
- Agent and Agentless tabs do not appear on the Overview page.
- Enterprise onboarding

Deployment of IPS as a RADIUS Proxy

In environments with many distributed users, it can be difficult or impossible to maintain a centralized database of users. Using RADIUS proxy, IPS RADIUS server can forward authentication requests from a network access device (NAD) to an external RADIUS server.

You can configure IPS to proxy RADIUS inner or outer authentication to an external RADIUS server. Proxying inner or outer authentication gives you the flexibility to direct requests for authentication through whatever realm is most appropriate for each user.



The authentication process when using an external authentication server is described below:

1. The endpoints connect to switch.
2. The switch receives the request and starts the RADIUS authentication with IPS.

3. IPS receives the request and then forms another RADIUS request and forwards it to the external RADIUS server.
4. If authentication succeeds the IPS assigns the user the appropriate roles, and then passes the associated RADIUS attributes back to the access device.

With RADIUS proxy enabled, IPS acts as a simple relay agent and does not participate in the accounting and authorization process. You must configure all attributes for authenticator configuration on the external RADIUS server.

You can specify the outer or inner proxy as follows:

- Outer proxy requires that the external RADIUS server presents a certificate to the supplicant. The result is a secure tunnel between the supplicant and the external server.
- Inner proxy uses the IPS certificate to establish the secured tunnel, but relays the supplicant authentication data to the external RADIUS server. The secured tunnel is established between the supplicant and IPS. The data passes between the IPS and the external RADIUS server in clear text.

Configuring 802.1X on IPS

This section covers the configuration for 802.1X authentication. It involves configuring the various elements necessary for performing 802.1X authentication between the endpoint and IPS.



802.1X authentication is also supported on external port. As a prerequisite, the Admin must enable Global Setting with Auth Traffic Control option. For configuration procedure, see "[AAA Traffic Management](#)" on page 551

Configuring Authentication Protocol Set

Authentication protocol is a method of defining how endpoints are authenticated through IPS. IPS supports a set of authentication protocols. You can configure sign-in policy with combination of authentication protocol set and associate them with realms to determine how endpoints connect and authenticate using 802.1X. The IPS supports a variety of EAP and non-EAP authentication methods to allow you to determine how endpoints authenticate. For example, you can use the default EAP methods with Pulse Client, or you can use different methods to permit authentication with different endpoints, such as non-Pulse Secure 802.1X supplicants and IP phones.

For IPS agents (Pulse Client and Host Checker agentless access), authentication is supported through EAP-TTLS and EAP-PEAP as the outer protocols and EAP-JUAC (a proprietary protocol) by default.

EAP-TTLS first authenticates the server and sets up an encrypted Transport Layer Security (TLS) tunnel for secure transport of authentication information. Within the TLS tunnel, a second authentication protocol is used to authenticate the user. EAP-TTLS is the “outer” authentication, while the second protocol is the “inner” authentication.

The following is a list of supported EAP types:

EAP-PEAP uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL / TLS tunnel between the client and the authentication server. The exchange of information is encrypted and stored in the tunnel ensuring the user credentials are kept secure.

- EAP-JUAC is a proprietary protocol that enables host check, firewall provisioning, and IP address restrictions.
- EAP-TTLS uses server-side certificates to set up authentication between clients and servers.
- EAP-SoH allows the endpoint to exchange state of health messages with IPS to assess endpoint qualification for passing Statement of Health rules in a Host Checker policy. It is used only with Windows native 802.1X supplicants.
- EAP-Generic Token Card (EAP-GTC) supports the use of authentication tokens.
- PAP supports the exchange of plaintext passwords.
- CHAP support includes MS-CHAP, MS-CHAPv2, EAP-Message Digest 5 (EAP-MD5), and EAP-MS-CHAPv2
- Password Authentication Protocol (PAP) with plain-text passwords.
- EAP Transport Layer Security (EAP-TLS) allows non-Pulse Secure 802.1X supplicants to authenticate through a certificate authentication server.

IPS supports these authentication protocols as non-tunneled authentication methods as well as inner authentication methods, depending on the policies that you configure. You can configure protocol sets with or without EAP, with the exception of MD5, EAP-GTC, EAP-TLS, and EAP-SOH, which are supported only for EAP. To use EAP-SOH, you must use EAP-PEAP as an outer authentication protocol.

If you use a protocol set with inner and outer authentication, both protocols must match the inner and outer protocol that is configured for the endpoint.

IPS uses two default preconfigured protocol sets.

- 802.1X protocol set that is used by default with IPS agents.
- 802.1X-phones protocol set that is used for authenticating 802.1X IP phones.

Third-party supplicants cannot use the preconfigured 802.1X protocol set. For example, some switches can request authentication using CHAP, or EAP-MD5-Challenge. For such devices, you must define an authentication protocol set.

Outer	Inner	Basis	Usage recommendation
PAP [1]	n/a	Password	Local auth server, Active Directory, LDAP [2] Cisco switch authentication
CHAP [1]	n/a	Password	Captive portal or authentication of switch administrators for HP ProCurve switch
EAP-MD5-Challenge [1]	n/a	Password	Captive portal or authentication of switch administrators, some IP phones
MS-CHAP [1]	n/a	Password	
MS-CHAP-V2 [1]	n/a	Password	
EAP-MS-CHAP-V2 [1]	n/a	Password	
EAP-GTC [1]	n/a	Token	
EAP-TLS	n/a	User Certificate	802.1X supplicant, some IP phones

Outer	Inner	Basis	Usage recommendation
EAP-PEAP			Non-Pulse Secure 802.1X supplicant
	EAP-MS-CHAP-V2	Password	Local or Active Directory server
	EAP-GTC	Token	802.1X supplicant
	EAP-TLS	User Certificate	
	EAP-JUAC	Various	Pulse Client
	EAP-SOH	System Health	Windows supplicant with Statement of Health Host Checker policy
EAP-TTLS			Pulse Client, other supplicant
	PAP		LDAP authentication server
	CHAP		
	EAP-MD5-Challenge		
	MS-CHAP		
	MS-CHAP-V2		
	EAP-MS-CHAP-V2		Local or Active Directory server
	EAP-GTC		802.1X supplicant
	EAP-JUAC		Pulse Client

The following additional information is intended to help you understand the protocols that have been implemented for our 802.1x solution:

- Pulse always uses EAP-TTLS/EAP-JUAC.
- EAP-TTLS, EAP-PEAP, and EAP-TLS are based on TLS and therefore secure. We recommend protecting other protocols by putting them into an EAP-TTLS or EAP-PEAP tunnel, if the supplicant supports one of these tunnels.
- With LDAP, there are 3 protocol possibilities:
 - If the LDAP server is also an Active Directory server, configure the server on IPS as an Active Directory server, not as an LDAP server. On IPS, PEAP-MS-CHAP-V2 is enabled by default. You can also enable MS-CHAP and MS-CHAP-V2 if necessary.
 - If passwords in the LDAP server are stored irreversibly hashed, CHAP family protocols will not work, only PAP and TTLS-PAP will work. On IPS TTLS-PAP is enabled by default. You can enable PAP if required, but this is the least secure protocol.
 - Some LDAP servers allow you to store the passwords in clear text or reversibly encrypted. In this situation, all the CHAP family protocols will work.

During RADIUS authentication, if a user's password has expired then the user is prompted to change the password if the protocol is:

- EAP-MSChapV2
- PEAP with EAP-MSChapV2
- TTLS with EAP-MSChapV2
- TTLS with Non-EAP MSChapV2
- Plain Non-EAP MSChapV2
- EAP-JUAC

The following table summarizes additional usage guidelines.

- Password- The protocols that support password changing on IPS include JUAC, MS-CHAP-V2, EAP-MS-CHAP-V2, and EAP-GTC. If you use CHAP, PAP or MS-CHAP for a Layer 2 connection (for example, with an Active Directory Server), password changing is not supported through IPS.
- Expired passwords- You can direct users with expired passwords to a Web interface to access a default VLAN to allow users to log in with a clear text password and change their password.

- Password restrictions- Password restrictions (for example, password length) cannot be enforced if you use the CHAP family protocols for authentication.
- Default protocols for Pulse- The 802.1X protocol set is used by default for endpoints that connects Pulse Client. If you disable the JUAC protocol (a proprietary protocol) on Pulse Client IPS and Pulse have only the features of a standard non-Pulse Secure supplicant.

To configure an authentication protocol set:

1. Select **Authentication > Signing In > Authentication Protocols**.

- The default 802.1X protocol set is configured with EAP-TTLS and EAP-PEAP as primary (outer) authentication protocols.



- EAP-JUAC, EAP-MSCHAP- V2 are used as inner authentication for EAP-PEAP.
- EAP-JUAC, PAP, MSCHAP- V2, EAP-MS-CHAP-V2, or EAP-GenericTokenCard are used as inner authentication for EAP-TTLS.

2. To create a new protocol set, click **New Authentication Protocol**, or select the check box beside the existing 802.1X protocol set and click **Duplicate**.

3. Enter a name, and optionally a description for the new authentication protocol set. You select the protocol set by name when you create a sign-in policy.

4. Under Authentication Protocol, select authentication protocol(s) from the Available Protocol list. Click **Add**.
5. For non-tunneled protocols, create an authentication protocol set, which includes CHAP, PAP or EAP-MD5 Challenge.
6. If you select EAP-PEAP as the main authentication protocol, under PEAP select an inner authentication protocol from the Available Protocol list. Click **Add**.
7. If you select EAP-TTLS as the main authentication protocol, under TTLS select an inner authentication protocol from the Available Protocol list. Click **Add**.



If you are using inner RADIUS proxy, do not select an inner protocol with EAP-PEAP or EAP-TTLS.

8. Click **Save Changes** to save your selections. When you configure a sign-in policy, you associate this authentication protocol set with an authentication realm.

Creating and modifying the sign-in policy

Sign-in policies define both the URLs that users and administrators use to access the network and to view the sign-in pages. IPS has two types of sign-in policies—one for users and one for administrators. When you configure sign-in policies, you associate realms, sign-in pages, and URLs that are provided for users when they first log in.

To modify the authentication protocol set used by a specific authentication realm:

1. Select **Authentication > Signing In > Sign-In Policies** and click **New URL**.

New Sign-In Policy

User type: Users Administrators

Sign-in URL: Format: -host-i-qaath- Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: To create or manage pages, see Sign-In pages.

Authentication realm

Specify what realms will be available when signing in.

Available realms	Authentication protocol set	
<input type="text" value="Cert Auth"/>	<input type="text" value="- Not applicable -"/>	<input type="button" value="Add"/>

If more than one realm appears above, Odyssey Access Client or the Policy Secure sign-in page will ask the user to choose. Other endpoints cannot choose a realm; the Policy Secure will assign the first suitable realm from the list. If no realms appear above, sign-in will fail.

User may specify the realm name as a username suffix
When this option is selected, the username suffix will be used to specify a realm.

Remove realm suffix before passing to authentication server
When this option is selected, the username suffix will be stripped from the username prior to authenticating with an authentication server.

Fail if suffix does not match any of the realms
When this option is selected, the user should provide one of the realm as suffix. If not, the user will be denied sign-in.

2. Under Authentication realm, add a new realm or modify an existing realm.
3. Select the desired authentication protocol set.
4. Click **Save Changes**.

Configuring a Location Group

Location groups let you organize or logically group network access devices by associating the devices with specific sign-in policies. Sign-in policies provide a way to define and direct independent access control policies with the network. For example, you can create location group policies to logically group the switch/WLC in each building at a corporate campus. You can also use location group policies to specify a special realm for MAC address authentication.

To configure a location group:

1. Create a sign-in policy to associate with the location group.
2. Select **Endpoint Policy > Network Access > Location Group**.

3. On the New Location Group page, enter a name to label this location group and optionally a Description.
4. For Sign-in Policy, select the sign-in policy associate with the location group.
5. Click **Save Changes**.



Location groups allows you to block Layer 2 endpoints in specific locations from using particular authentication protocols, realms, and roles. For example, you can block endpoints in insecure locations from accessing sensitive roles. However, RADIUS clients should not be placed in insecure locations. To ensure that RADIUS clients are not compromised and do not violate these policies, all the network RADIUS clients should be securely protected.

Configuring the network access device as a RADIUS Client

A RADIUS client policy specifies the information required for an 802.1X network access device to connect as a RADIUS client of the IPS.

When you select the device's make and model in a RADIUS client policy, you are selecting a dictionary file that contains the vendor-specific attributes (VSAs) for that device. Whenever IPS receives a RADIUS packet from that device, it consults the dictionary file for any nonstandard attributes that it encounters in the packet. If you do not know the make and model of a device, you can use the standard RADIUS attributes by choosing the Standard RADIUS setting in a RADIUS client policy.

In addition to the configuration on IPS, you must configure the NAD with information about IPS, including:

- IP address
- Shared secret specified in the RADIUS client policy for the device

To configure a RADIUS client:

1. Select **Endpoint Policy > Network Access > RADIUS Client**.
2. Click **New RADIUS Client**.

▼ RADIUS Client

🟢 Cisco WLC 10.204.88.244 successfully updated.

* Name: Cisco WLC 10.204.88.244 Label to reference this RADIUS Client

Description:

* IP Address: 10.204.88.244 IP Address of this RADIUS Client

* IP Address Range: 1 Number of IP Addresses for this RADIUS Client

* Shared Secret: RADIUS shared secret

Key Wrap Key Wrap (Support for RFC 6218)

* Key Wrap Format: ASCII Key Wrap Format

* Key Encryption Key(KEK): Key Encryption Key(KEK), size should be 16 bytes

* Message Authentication Code Key(MACK): Message Authentication Code key (MACK), size should be 16 bytes to 64 bytes

* Make/Model: Airespace To manage make/model, see the [RADIUS Vendor](#)

* Location Group: Default To manage groups, see the [Location Group](#)

▼ Dynamic Authorization Support

Support Disconnect Messages Disconnect Message Support

3. On the RADIUS Client page, enter a name to label the RADIUS client. You can assign any name to a RADIUS client entry, use the device's SSID or IPv4/IPv6 address to avoid confusion.
4. (Optional) Enter a purpose or description of the configuration so that other users are aware of it.

5. Enter the IPv4/IPv6 address of the switch.



If you specify the Switch Address as IPV6, IPS will allow Pulse Client to connect only using Client's IPv6 address in 802.1x Connection Type.

6. (Optional) **For IP Address Range**, enter the number of IP addresses in the IP address range for the switch/WLC, starting with the address you specified for IP Address. You can specify a range up to a maximum of 32,768 addresses.
7. For **Shared Secret**, enter the RADIUS shared secret. A RADIUS shared secret is a case-sensitive password used to validate communications between IPS and NAD. IPS supports shared secrets of up to 127 alphanumeric characters, including spaces and the following special characters:

~!@#%\$%^&*()_+|\=-'{}[]:~";<>?/.,

8. For **Make/Model**, select the make and model of the NAD. The make/model selection tells IPS which dictionary of RADIUS attributes to use when communicating with this client. Note that **Ruckus Request Password** needs to be configured only for **SmartZone Guest Access**.
9. (Support for RFC 6218: Cisco/Airespace Switches). If you are configuring a new RADIUS authentication server and want to enable AES key wrap, which makes the shared secret between the controller and the RADIUS server more secure, follow these steps:

- Enable the Key Wrap checkbox.
- From the Key Wrap Format drop-down list, choose ASCII or HEX to specify the format of the AES key wrap keys: Key Encryption Key (KEK) and Message Authentication Code Key (MACK)
- Enter the 16-byte KEK used for encrypting the key generated by the server
- Enter the 16-64 bytes MACK used for authenticating the messages.



AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.

10. For **Location Group**, select the location group to use with this NAD.

11. Under **Dynamic Authorization support**, Select the **Support Disconnect Messages** check box to send disconnect messages to supplicants if access is no longer authorized. If this check box is selected, a disconnect request is sent to the NAD any time a session is deleted. IPS can also send disconnect messages upon a role event that includes a VLAN change or a change in RADIUS attributes.
12. Select **Support CoA Messages** to enable CoA messages and disconnect messages support for the client. Ensure that Pulse Client is configured with EAP-JUAC in EAP-TTLS inner protocol as most preferred protocol.
RADIUS CoA feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. Using the existing session, RADIUS CoA allows devices to change the VLAN/ACL for the endpoint based on roles. CoA works on role mapping associated with every user. As the device state changes, the user is put in to various roles based on the Host Checker assessment or compliance check. During the dynamic assessment, CoA requests such as filter-id or any other return attributes that suites the role is sent to the NAD to provide the required access for the device. IPS receives CoA-NAK request if the NAD is not able to apply filter-id or any other return attributes.
13. (Optional) Enter a new **Dynamic Authorization Port** (Default port is 3799). The default port might vary depending on the manufacturer. NAD listens to UDP port to receive RADIUS CoA messages from IPS.
14. Click **Save Changes**.

Configuring Role and Role Mapping

IPS access management framework evaluates authentication requests to match endpoints to roles. You must configure user roles for the various types of endpoints authenticated.

To create a user role:

1. Select **Users > User Roles**.
2. Click **New Role**.

- Complete the name and description configuration and then save the configuration.

User Roles > New Role

New Role

Name:

Description:

Options

Session and appearance options are specified in Default Options. Check the following if this role should override these defaults.

- Session Options
- UI Options
- Odyssey Settings for Access
- Odyssey Settings for Preconfigured Installer
- Enable Guest User Account Management Rights

Save Changes

- Click **Agent** and deselect agent options and then save the configuration.

User Roles > Users > Agent > General

General

General Agent Agentless

General Odyssey Settings

Options

- Install Agent for this role
- Enable Host Enforcer

Note:(Odyssey Access Client only) By default, if you enable Host Enforcer on a role, all traffic is blocked for users mapped to this role. Make sure you create Host Enforcer policies on the "Resource Policies>Host Enforcer" page to allow particular traffic for this role. Host Enforcer policies that apply to this role:

- Access control

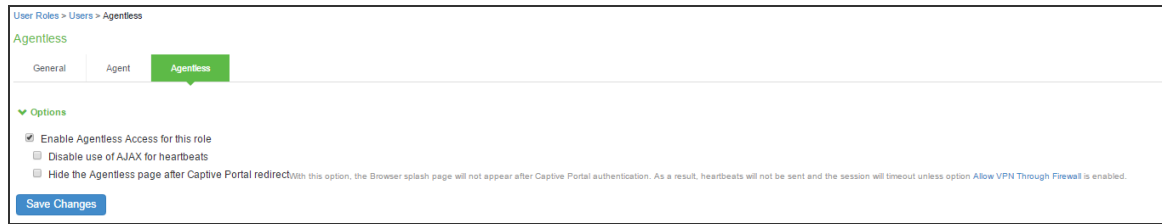
Session scripts

Windows: Session start script
This script is executed after the session has started.
Script Location:

Windows: Session end script
This script is executed after the session has ended.
Script Location:

Save Changes

- Click **Agentless** and enable agentless access and then save the configuration.



Role mapping rules define how endpoints are assigned to roles.

To configure the role mapping rules for User Realms:

- Select **Users > User Realm**.
- Click **New** to display the User Realm configuration page and create a user realm.
- Click the **Role Mapping** tab to display the role mapping configuration page for the realm.
- On the role mapping configuration page, click **New Rule** to display the role mapping rule configuration page.
 - (Optional) For Name, enter a name to label this role mapping rule.
 - Select the rule from the Rule based list and provide the appropriate details.
 - Select the appropriate role and click **Add**.
- Click **Save Changes** to save the configuration.

Configuring RADIUS Attributes Policies

This section describes the configuration information for RADIUS return attributes policy that is applied on switch, request attribute policy, which can be used along with sign-in policies for realm selection, policy realm restrictions, and authentication/accounting reporting for RADIUS authentication events.

Configuring RADIUS Return Attributes

RADIUS attributes policies sends the return list of attributes to an 802.1X switch. For example, you can specify which VLAN endpoints must be used to access the network. You can also configure other functions on a NAD's port based on the role assigned to the user who is currently using that port. For example, a Switch might let you use return list of attributes to configure Quality-of-Service (QoS) functions (Bandwidth or Priority) on the device's port based on the current user's role.

A return list is a set of attributes that IPS returns to the NAD after authentication. The return list usually provides additional parameters that the NAD needs to complete the connection. Return list attributes are authorization configuration parameters.

In the RADIUS attributes policy, you can select RADIUS attributes by name from a predefined list. For each attribute, you specify values using strings or numbers. By default, IPS sends a session timeout value on all RADIUS accepts that is equal to the timeout value of the configured session length. You can bypass the default timeout.

To configure a RADIUS attributes policy:

1. Select **Endpoint Policy > Network Access > RADIUS Attributes**.

2. Click **New Policy**.

Network Access > Radius Attributes > RADIUS Return Attributes > Full Access Policy

Full Access Policy

General

* Name: Full Access Policy Required: Label to reference this policy.

Description:

Location Group

Location Groups
Specify the Location Group for which this policy applies.

Available Location Groups: Default, Guest, Cert Auth, Guest Wired, HP Test Location

Selected Location Groups: Cisco Test Location

Selected Radius Clients
Below list is populated dynamically based on the selected Location Groups

Vendor (Manufacturer)	Client Details
Cisco Systems	Cisco 3850 ,

Access Control Policy Settings

Select below option to control the access level for the device/user connecting to the network.

Provide full Access (Open Port) Note: Selecting this option will result in opening the port without any restrictions

Control the Access Note: Selecting this option enables control of the device or user access

Access can be controlled using the VLAN Id, ACLs and Radius Return Attribute settings below

Control using VLAN Id: 80 (1 - 4094) Note: This option is used for assigning devices to corresponding VLAN on the switch

Specify the PPS interface to which end points will connect while they are assigned to above VLAN

Automatic Internal External

Control access using Access Control List (ACL) settings (Supported only for Cisco, Juniper, HP)

Specify the ACL mode for controlling the device access

ACL Name:

ACL Rule(s) Note: Specify the ACL rules to be applied on the switch

Delete ↑ ↓

Protocol	Destination IP / Network	Destination Port	Action
ip			permit
<input type="checkbox"/> tcp	10.204.89.245	443	permit
<input type="checkbox"/> tcp	10.204.89.246	443	deny

Control access using Radius Return Attributes Note: These attributes are sent to switch for controlling the access

Delete ↑ ↓

Return Attribute	Radius Auth Server Attribute Value	Auth Server Catalog Attribute Value	Value
Filter-Id	-none-	-none-	
<input type="checkbox"/> Filter-Id	-none-	-none-	PERMIT-ALL.in

Add Session-Timeout attribute Note: This will send session timeout attribute equal to session lifetime

Specify the action that needs to taken for the device upon expiration of session timeout on the switch

Terminate the session Re-authenticate the session

Roles

Select the roles to which this policy is applicable

Any Role Selected below Other than selected below

Available roles: Agentless_full_role, Agentless_rem_role, Compliant Role, Eng, Guest

Selected roles: ENGG

Save Changes Cancel

NOTE: Any changes to this page results in termination of existing L2 connections and triggers reconnections.

3. On the New Policy page, enter a name for the policy.
4. (Optional) For Description, enter a description for the policy.
5. Under Location Group, select the location groups to which you want to apply this policy, and click **Add**. To apply the policy to all location groups, do not add any location groups and use the default setting (all) listed in the Selected Location Groups list. The selected Radius clients table is dynamically updated based on the selected Location Groups.

6. Under Access Control Policy Settings, select from the following options:

- **Provide full Access (Open Port)**-Check this option if you do not want to assign endpoints to a VLAN or return any RADIUS attributes. Selecting this check box disables all other RADIUS Attributes options.

- **Control the Access**-Select this option to control access using VLAN ID, ACLs and RADIUS return attributes.

Control using VLAN Id: Enter the VLAN ID (1-4094) used for assigning devices to corresponding VLAN on the switch.

- For Interface, specify IPS network interface that endpoints affected by this policy to use to connect to IPS:
- **Automatic (use configured VLANs)**-Select this option to use VLAN tagging. You must also connect the internal interface to the trunk port on a VLAN-enabled Switch that sees all the VLAN traffic.
- **Internal**- Select this option if the endpoints using this RADIUS attributes policy should use the IP address of the internal interface.
- **External**-Select this option if the endpoints on the configured VLAN should use the IP address of the external interface.

Control access using Access Control List (ACL) settings (Supported only for Cisco, Juniper, HP)

- Specify the ACL Name for controlling the device access or specify the ACL Rule to be applied on the Switch.
- Select the Protocol (IP/TCP/UDP/ICMP), Destination IP/Network Mask, Destination Port, Action (Permit/Deny) and Click **Add**.



The supported RADIUS clients for ACL mode are Cisco, Juniper, and HP switches. If there are any unsupported clients listed in the Supported RADIUS client table then the ACL configuration will be disabled.

Control Access using Radius Return Attribute-Select this option to specify the return attributes you want sent to the Switch/WLC.

- Select the return attribute to send from the attribute list. Enter the value for the selected attribute and then click **Add**.
- You can specify multiple return attributes and values for this policy.

- To rearrange the order in which you want to send the return attributes, select the check box next to the attribute name and then click the up or down arrow.
- To delete an attribute, select the check box next to the attribute name then click Delete.



If both (user/policy) have the same attributes, preference will be given to User attribute values.

Add Session-Timeout attribute-Select this option to specify the action (Terminate the session or reauthenticate the session) taken upon on the expiration of session timeout.

7. Under Roles, specify:

- **Any role**-To apply the policy to all users.
- **Selected roles**-To apply this policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
- **Roles other than those selected below**-To apply this policy to all users except for those who map to the roles in the Selected roles list. You must add roles to this list from the Available roles list.

8. Click **Save Changes**.



VLAN change using CoA is not supported with Cisco Switches. It is recommended to use RADIUS disconnect for VLAN change.

Name	ACL Settings	Attributes	Location Group	Interface	Applies to role
1. Full Access Policy	ACL Rule=Protocol tcp, Destination IP: 10.204.89.245, Destination Port: 443, Action: permit ACL Rule=Protocol tcp, Destination IP: 10.204.89.246, Destination Port: 443, Action: deny	VLAN=80 Filter-Id=PERMIT-ALL in	Cisco Test Location	AUTO	ENGG

Example configuration for parsing ACL rule name (HP, Cisco, and Juniper)

IPS ACL rule configuration	tcp 10.xx.xx.x 443 Permit
HP 2920 expansion	HP-nas-filter-rule=permit in tcp from any to 10.xx.xx.x 443

IPS ACL rule configuration	tcp 10.xx.xx.x 443 Permit
Cisco 3850 expansion	ip:inacl#100=permit tcp any host 10.xx.xx.xxx eq 443
Juniper - EX 2200 expansion	Juniper-Switching-Filter='Match Destination-ip 10.xx.xx.x Ip-protocol 6 Destination-port 443 Action allow'

Example configuration for parsing ACL name (HP, Cisco, and Juniper)

Vendors	Cisco	HP	Juniper
RADIUS VSA	filter-id	filter-id	filter-id
Example- RADIUS VSA value	<ACL-NAME>.in	<ACL-NAME>.in	ACL-Name

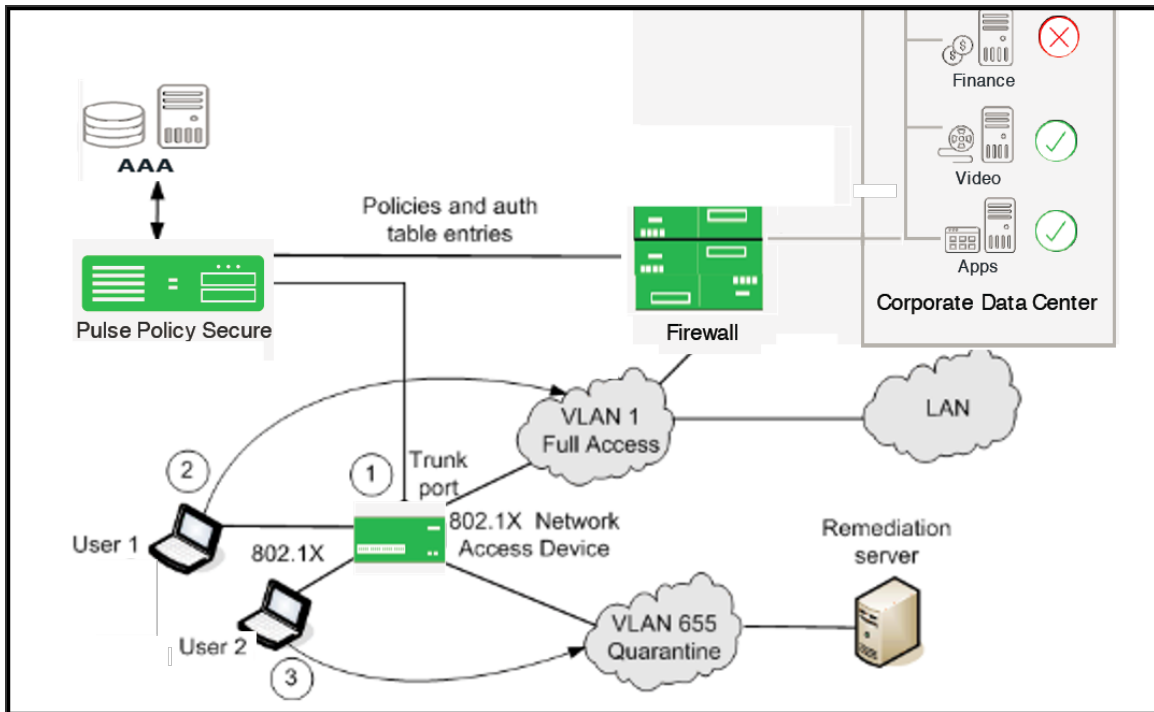
Example: RADIUS Attribute Policies

You can configure RADIUS attributes in the IPS to send return list attributes to an 802.1X network access device. For example, you can specify which VLAN the endpoint must use to access the network. You can also configure other functions on the network devices port based on the role assignment. For example, a particular Switch might let you use return attributes to configure QoS functions (bandwidth, priority, or both) on the device port based on the user role.

The example illustrates a RADIUS attribute policy to specify VLANs for endpoints, using the following steps:

- If you are using more than two VLANs, connect IPS internal interface to the trunk port on a VLAN-enabled switch that detects all the VLAN traffic.
- You can also configure a RADIUS attributes policy with the Automatic setting, which enables IPS to take advantage of VLAN tagging. When connected to a trunk port on a VLAN-enabled switch, IPS detects traffic from all VLANs.
- You can also configure routing on the network to enable endpoints to access IPS over the network. In this case, you must configure RADIUS attributes policies with the VLAN IDs you are using for endpoints, but you do not need to configure any VLAN ports on IPS.

The following figure illustrates an example of using a RADIUS attributes policy to specify VLANs for endpoints.



- If the user 1 is authenticated and the endpoint complies with Host Checker security policies, then the user is assigned a role on the Full Access VLAN that allows full network access and access to protected resources.
- If user 2 is authenticated but the endpoint does not comply with Host Checker security policies. The user is assigned a role on the Quarantine VLAN that only allows access to a remediation server.

Example: Configuring various RADIUS Return Attribute Policies

Configuring VLAN Assignment using RADIUS return Attribute Policy

This configuration describes how to send VLAN assignment to the Switch/WLC by returning RADIUS attributes.

1. Select **Ivanti Policy Secure > Network Access > RADIUS Return Attributes**.
2. Under Access Control Policy Settings, select Control the **Access > Control using VLAN ID**.
3. Specify a **VLAN ID**.

Configuring VLAN Assignment along with other RADIUS return Attributes Policies

This configuration describes how to send VLAN assignment and other attributes to the Switch/WLC by returning RADIUS attributes.

1. Select **Ivanti Policy Secure > Network Access > RADIUS Return Attributes**.
2. Under **Access Control Policy Settings**, select Control the **Access > Control using VLAN ID**.
3. Specify a VLAN ID.
4. Select **Control Access using Radius Return Attributes**.
5. Select the attribute you want to return from the Attribute list.
6. For Value, specify an attribute value.

Configuring Filter-ID using RADIUS Return Attribute Policy

This configuration describes how to send Filter-ID to switch/WLC by using the Filter-ID return attribute.

1. Select **Endpoint Policy > Network Access > RADIUS Return Attributes**.
2. Under Access Control Policy Settings, select Control Access using Radius Return Attributes.
3. Select **Filter-ID** from the Attribute list.
4. For value, specify the policy name.
5. Configure the filter on the NAD.

Configuring VLAN Assignment in a multi-vendor Switch Environment

This configuration describes how to send VLAN assignment in a multi-vendor switch environment that includes switch/WLC from different vendors. For example, you might have one type of switch that supports RADIUS tunnel attributes only, a second type of switch that supports the Filter-ID return attribute only, and a third type of switch that supports both.

1. Select **Endpoint Policy > Network Access > Location Group** and create a location group policy for each type of NAD.
2. Create a location group policy for switches that support RADIUS tunnel attributes only.

3. Create a second location group policy for switches that support the Filter-ID return attribute only.
4. Create a third location group policy for switches that support both RADIUS tunnel attributes and the Filter-ID return attribute.
5. Select **Endpoint Policy > Network Access > RADIUS Client**. Then, follow these steps to create a RADIUS client policy for each type of NAD and associate each RADIUS client policy with the appropriate location group.
6. Create a RADIUS client policy and specify a make/model for Make/Model that supports the RADIUS tunnel attributes. Associate this policy with the location group policy for switches that support RADIUS tunnel attributes only.
7. Create a second RADIUS client policy and specify a make/model that supports the Filter-ID return attribute. Associate this policy with the location group policy for switches that support the Filter-ID return attribute only.
8. Create a third RADIUS client policy and specify a make/model that supports the both RADIUS tunnel attributes and the Filter-ID return attribute. Associate this policy with the location group policy for switches that support both RADIUS tunnel attributes and the Filter-ID return attribute.
9. Select **Endpoint Policy > Network Access > RADIUS Attributes** and then follow these steps:
 - Create a RADIUS Attributes policy that specifies only the VLAN option and a value for VLAN ID. Associate this policy with the location group policy for switches that support RADIUS tunnel attributes only.
 - Create a second RADIUS Attributes policy that specifies only the Filter-ID option from the Attribute list and a policy name for Value. Associate this policy with the location group policy for switches that support the Filter-ID return attribute only.
 - Create a third RADIUS Attributes policy that specifies both the VLAN option and a value for VLAN ID, and the Filter-ID option with a policy name for Value. Associate this policy with the location group policy for switches that support both RADIUS tunnel attributes and the Filter-ID return attribute.

Configuring RADIUS Request Attribute Policies

RADIUS request attribute policies allows you to enforce the authentication requests based on information in the RADIUS packet. RADIUS request attribute policies consist of rules. Each rule consists of one attribute and some number of values. The type of value depends on the type of rule chosen. For example, if you select a rule with the User-Name attribute, you enter a string.



- RADIUS request attribute policy names must be unique.
- Each request page includes guidance on what type of value is expected.

If you select a rule with the Login-IP-Host attribute, you enter an IP address and an optional netmask. The default netmask value is 255.255.255.255. The value of the attribute must fall within the specified IP address and netmask to pass the policy.

The RADIUS Access-Request attribute policy performs two tasks:

- Determines communication with the RADIUS client, indicating that the specified attributes must be sent in the Access-Request message.
- Parses the attribute-value pairs that are sent in the Access-Request message against the allow/deny rules you configure. The result of rules processing can be enforced in a realm restriction.

To configure a RADIUS Request attribute policy:

1. Select **Endpoint Policy > Network Access > RADIUS Attributes > Request Attributes** to display the configuration summary page.
2. Click **New** to display the policy configuration page.

Request Attribute	Value	Allow/Deny

3. Specify a policy name and description.

- Under Rule Settings, select a RADIUS Access-Request attribute and click Add to display the rule configuration page.

Network Access > RADIUS Request Attributes > RADIUS Request Attribute Policy

RADIUS Request Attribute Policy

Use this policy to restrict the users with these RADIUS Request Attributes

▼ RADIUS Request Policy

* Policy Name: Label to reference this RADIUS Request Attribute Policy.

Description:

▼ Rule Settings

ARAP-Password To manage attributes, see the RADIUS Dictionary

Request Attribute	Value	Allow/Deny

- Complete the rule configuration as described below.

Settings	Guidelines
Add	Specify values or a pattern for rule matching. The system parses wildcards and value expressions as follows:
	String-An asterisk (*) matches multiple characters and a question mark (?) matches a single character.
	Integer-An asterisk (*) matches any value. You can use a hyphen to specify a range of values, for example 1-99 .
	Hexadecimal-An asterisk (*) matches any value.
	Click Add again to add more attribute values, as necessary. The result of adding multiple values is a comma-separated list.
Allow / Deny	Select Allow to permit access to matching sessions. Select Deny to deny access to matching sessions.

6. Save the rule configuration and return to the policy configuration page.

Network Access > RADIUS Request Attributes > RADIUS Request Attribute Policy

RADIUS Request Attribute Policy

Use this policy to restrict the users with these RADIUS Request Attributes

▼ RADIUS Request Policy

* Policy Name: Label to reference this RADIUS Request Attribute Policy.

Description:

▼ Rule Settings

ARAP-Password To manage attributes, see the RADIUS Dictionary

Request Attribute	Value	Allow/Deny
<input type="checkbox"/> NAS-Port	30,34	Allow

Configuring a RADIUS Request Policy Realm Restriction

RADIUS request attribute policies can be assigned with a realm restriction. Any authentication request that comes from a realm with attribute policy requirements sends the RADIUS attributes specified in the policy, otherwise the authentication request is not granted. If multiple rules are configured in a policy, then all rules in the policy must pass otherwise the authentication fails.

If a user authentication fails based on the RADIUS request attribute policy, a user event log message is displayed. Debug logs allow the administrator to determine that a user met the policies, or indicate that the user failed a RADIUS return attribute policy.

To configure a RADIUS Request realm restriction:

1. Select **Endpoint Policy > Network Access > RADIUS Attributes > Request Attributes** to display the configuration summary page.
2. Click **New** to display the policy configuration page.
3. Complete the configuration as described in the following table.

4. Click **Save**.

Settings	Guidelines
Policy list	Use the Add and Remove buttons to create a policy list. The available policies are populated by the RADIUS request policies configured in the prior procedure.
Allow access to realm if any one of the selected policy is passed.	This option determines what happens when multiple policies match. Select this option to allow access to the realm if any of the matching policies allow access (Ignoring any matching deny policies). Do not select this option if you want to deny access if one of the matching policies deny access (Ignoring any matching allow policies).

Configuring RADIUS Attribute Logging

You can configure IPS to enable or disable authentication reporting for RADIUS authentication events. Using this feature you can obtain a granular record of authentication attempts using configurable and detailed authentication reports.

You can selectively choose events to record based on both successful and unsuccessful authentication attempts. If you select an attribute to be recorded and the value is not present in the authentication request/response, an entry is made in the debug log and in the RADIUS log. You can also specify accounting log messages.

The byte limit for log entries is 2048. If a message exceeds the byte limit the last value is trimmed and an entry is made in the debug and RADIUS logs.

To configure RADIUS attribute logging:

1. Select **Endpoint Policy > Network Access > RADIUS Attributes > Attribute Logging**.

Network Access > Radius Attribute Logging

Radius Attribute Logging

RADIUS Dictionary | RADIUS Vendor | Location Group | RADIUS Client | **RADIUS Attributes** | SNMP Device | SNMP Enforcement Policies

Return Attributes | Request Attributes | **Attribute Logging**

▼ Authentication Success Log Attributes

Authentication Success Log Message

Available Attributes:

- 802.1P-Tag
- ACL-Name
- ARAP-Challenge-Response
- ARAP-Features
- ARAP-Password
- ARAP-Security
- ARAP-Security-Data
- ARAP-Zone-Access
- Acct-Authentic

Add ->

Remove

Selected Attributes:

- NAS-IP-Address
- NAS-Port
- NAS-Port-Type
- User-Name
- NAS-IPv6-Address
- NAS-Identifier
- Framed-IPv6-Address
- Framed-IPv6-Pool
- Framed-IPv6-Prefix

▲

▼

▼ Authentication Reject Log Attributes

Authentication Reject Log Message

Available Attributes:

- 802.1P-Tag
- ACL-Name
- ARAP-Challenge-Response
- ARAP-Features
- ARAP-Password
- ARAP-Security
- ARAP-Security-Data
- ARAP-Zone-Access
- Acct-Authentic

Add ->

Remove

Selected Attributes:

- NAS-IP-Address
- NAS-Port
- NAS-Port-Type
- User-Name
- Framed-IPv6-Route
- Framed-IPv6-Prefix
- Framed-IPv6-Pool
- Framed-IPv6-Address

▲

▼

▼ Accounting Log Attributes

Accounting Log Message

Available Attributes:

- 802.1P-Tag
- ACL-Name
- ARAP-Challenge-Response
- ARAP-Features
- ARAP-Password
- ARAP-Security
- ARAP-Security-Data
- ARAP-Zone-Access
- Acct-Delay-Time

Add ->

Remove

Selected Attributes:

- Framed-IPv6-Address
- NAS-IPv6-Address
- Framed-IPv6-Prefix
- User-Name
- Acct-Authentic
- NAS-Identifier
- NAS-Port
- NAS-IP-Address
- Framed-IP-Address

▲

▼

Save Changes

2. Select Authentication Success Log Message and Authentication Reject Log Message.

3. Select the **Accounting Log Message** option to specify the accounting log messages.
4. Select **Available attributes** from the lists, and click Add to populate the Selected Attributes lists.
5. Click **Save Changes**.



- To include the RADIUS accounting messages in user access logs, select **System > Log/Monitoring > User Access > Settings and enable RADIUS Accounting Messages**.
 - The order of RADIUS attributes in the user access log is based on the order you select the attributes from the RADIUS attributes logging page.
-

Verifying the RADIUS Request Attribute Policy Configuration

When a user authentication fails because it did not meet the requirements specified in the RADIUS request attribute policy, a user event log message is displayed that includes information about which policies the user met or failed.

To display the User Access log:

1. Select **System Log/Monitoring**.
2. Click the **User Access** tab.
3. Click the **Log** tab.

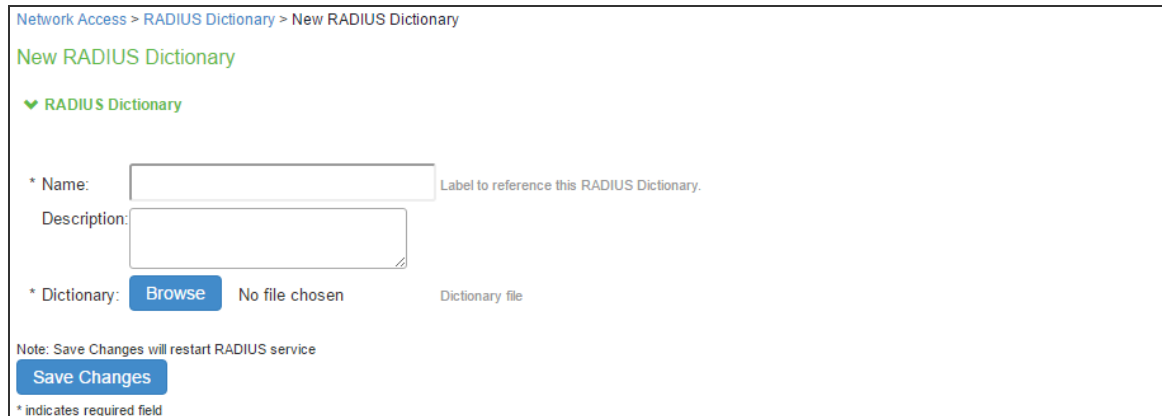
Verifying the RADIUS Dictionary

IPS supports many specific network access devices (NAD) by using its built-in standard RADIUS and vendor-specific, proprietary dictionary files. You can upload new dictionaries to add new RADIUS clients. IPS uses the dictionary files to store lists of RADIUS attributes, parse authentication requests, and generate responses.

To upload a new RADIUS dictionary:

1. Select **Endpoint Policy > Network Access > RADIUS Dictionary** to display the preconfigured dictionaries and their associated vendors.

2. Click **New RADIUS** dictionary.



The screenshot shows a web interface for creating a new RADIUS dictionary. The breadcrumb path is 'Network Access > RADIUS Dictionary > New RADIUS Dictionary'. The page title is 'New RADIUS Dictionary'. Below the title is a green checkmark icon and the text 'RADIUS Dictionary'. The form contains the following fields and controls:

- * Name:** A text input field with a placeholder 'Label to reference this RADIUS Dictionary.'
- Description:** A text area with a placeholder.
- * Dictionary:** A file selection control with a blue 'Browse' button, the text 'No file chosen', and 'Dictionary file'.
- Note:** 'Save Changes will restart RADIUS service'.
- Save Changes:** A blue button.
- * indicates required field** (at the bottom left).

3. Enter a Name and optionally a description for the new dictionary.
4. Click **Browse** to search for the dictionary file (.dct) on a local or connected drive, then click **Save Changes**. The uploaded dictionary is displayed on the main RADIUS Dictionary page, and in the Make/Model list on the RADIUS Client page.
5. Click **Save Changes**.



- You can only remove dictionaries that are not associated with a vendor.
- You can download any dictionary from the list, including preinstalled dictionaries. You can modify the downloaded dictionary and then upload it as a new make/model.

Verifying RADIUS Vendor List

RADIUS server contains a file with the list of manufacturers for the access devices, which communicate with the RADIUS server.

To verify the vendor and the associated dictionary on the RADIUS Vendor page:

1. Select **Network Access > RADIUS Vendor**.
2. Click **New RADIUS Vendor**, enter the name and then select the imported dictionary.

3. Click **Save Changes**.

Additional Configurations

Configuration Commands for Cisco Switch

The below example shows a sample configuration of 802.1X authentication on Cisco switch. Only sample commands are documented in this example. For more information, see Cisco documentation.

The configuration involves the following:

- Configuring IPS server as a RADIUS server in configuration mode.
- Configuring 802.1X on the switch port in configuration mode.

Configuring IPS server as a RADIUS server

The sample configuration below shows how to add IPS server as a RADIUS authentication and accounting server on Cisco switch.

You must execute the following commands in the CLI configuration mode.

```
--Execute this command to add IPS as a RADIUS server
```

```
radius server <RADIUS SERVER NAME>
```

```
*Note* IPS listens to both 1812/1813 and 1645/1646 ports. Default is 1645 and 1646.
```

```
address ipv4 <RADIUS SERVER IP> auth-port 1645 acct-port 1646
```

```
key <SHARED-KEY>
```

--Execute these commands to create a RADIUS Server Group, and associate your IPS appliances to the group.

```
aaa group server radius <RADIUS-GROUP>
server name <RADIUS SERVER NAME>
```

Note Repeat for every IPS Appliance.

--Execute these commands to turn on AAA

```
aaa new-model
aaa session-id common
aaa authentication dot1x default group <RADIUS-GROUP>
aaa authorization network default group <RADIUS-GROUP>
aaa authorization auth-proxy default group <RADIUS-GROUP>
aaa accounting send stop-record authentication failure
aaa accounting identity default start-stop broadcast group <RADIUS-GROUP>
aaa accounting update newinfo
```

-- Execute this command to configure RADIUS CoA

```
aaa server radius dynamic-author
client <RADIUS SERVER IP> server-key <SHARED-KEY>
auth-type all
ignore session-key
port 3799
```

Note Default is 1700

--Optional commands for DHCP snooping and IP device tracking for dACL or filter id attributes

```
ip device tracking
ip dhcp snooping
ip http server
ip http secure-server
```

Configuring 802.1x and MAC Authentication

The below example shows a sample configuration of 802.1X and MAC Address authentication on Cisco switch interface. You must execute the following commands in CLI configuration mode.

```
interface GigabitEthernet1/0/24
switchport access vlan 60
switchport mode access
```

--Execute this command to trigger re-authentication from IPS

```
authentication periodic
authentication timer reauthenticate server
```

--Execute this command for configuring 802.1X

```
access-session port-control auto
dot1x pae authenticator
```

```
--Execute this command for configuring MAC BYPASS
    mab
    spanning-tree portfast
    service-policy type control subscriber POLICY_Gi1/0/24
--POLICY_Gi1/0/24 is a policy map configuration. See the POLICY_MAP configuration for more
details.

--Specify the order of execution

    authentication order mab dot1x
    authentication priority dot1x mab
--Execute this command for viewing the status of the session on Cisco OS version 15.x and
above
    Show access-session interface gi-X/Y/Z detail
--Execute this command for viewing the status of the session on Cisco OS version 12.
    Show authentication session interface gi-X/Y/Z detail
```

POLICY_MAP configuration

```
--Execute this command to define POLICY_MAP configuration
--Define class-map Policies
class-map type control subscriber match-all DOT1X
match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
match method dot1x
match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
match method dot1x
match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all DOT1X_TIMEOUT
match method dot1x
match result-type method dot1x method-timeout
!
class-map type control subscriber match-all MAB
match method mab
```

```
!  
class-map type control subscriber match-all MAB_FAILED  
match method mab  
match result-type method mab authoritative  
--Define policy-map using class-map  
sh run | beg POLICY_Gil/0/24  
policy-map type control subscriber POLICY_Gil/0/24  
event session-started match-all  
    10 class always do-until-failure  
        10 authenticate using mab priority 10  
event authentication-failure match-first  
    5 class DOT1X_FAILED do-until-failure  
        10 terminate dot1x  
        20 authentication-restart 60  
    10 class MAB_FAILED do-until-failure  
10 terminate mab  
    20 authenticate using dot1x priority 20  
    20 class DOT1X_NO_RESP do-until-failure  
        10 terminate dot1x  
20 authentication-restart 60  
    40 class always do-until-failure  
        10 terminate mab  
        20 terminate dot1x  
        30 authentication-restart 60  
event agent-found match-all  
    10 class DOT1X_MEDIUM_PRIO do-until-failure  
        10 authenticate using dot1x priority 20  
event authentication-success match-all  
    10 class always do-until-failure  
        10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
```

Configuration Commands: EX Switch

```
set system services web-management http  
set system services web-management https system-generated-certificate  
--Execute this command for Employee Pulse dot1x  
set protocols dot1x authenticator interface ge-0/0/31.0  
protocols dot1x authenticator interface ge-0/0/32.0
```

--Agentless/Guest access

```
set protocols dot1x authenticator interface ge-0/0/35.0 mac-radius restrict
```

```
set firewall family ethernet-switching filter PERMIT-ALL.in term ALLOW_ALL from
destination-address 0.0.0.0/0
set firewall family ethernet-switching filter PERMIT-ALL.in term ALLOW_ALL then accept
set access radius-server 10.96.69.26 dynamic-request-port 3799
set access radius-server 10.96.69.26 secret "$9$TQ6ABIcevLEcK8XxdVqmPQ69"
set access radius-server 10.96.69.26 source-address 10.96.4.43
set access profile juniper-access-profile authentication-order radius
set access profile juniper-access-profile radius authentication-server 10.96.69.26
set access profile juniper-access-profile radius accounting-server 10.96.69.26
set access profile juniper-access-profile accounting order radius
```

Configuration Commands: Huawei Switch

The below example shows a sample configuration of 802.1X authentication on Huawei switch (S5720). Only sample commands are documented in this example. For more information, see Huawei documentation.

```
# Creation of VLAN
vlan batch 100 200

# Creation of dot1x profile
dot1x-access-profile name <dot1x-profile-name>
authentication trigger-condition dhcp

# Creation of authentication profile mapped to dot1x-access-profile
authentication-profile name <auth-profile-name>
dot1x-access-profile <dot1x-profile-name>
authentication mode multi-authen max-user 100

# For MAC auth (MAB), enable below 2 commands
mac-access-profile <Mac-profile-name>
authentication dot1x-mac-bypass

# Domain in which authentication happens
domain isp

# When Switch acts as CoA server, decoding of calling-station-id format has to be
specified.
radius-server authorization calling-station-id decode-mac-format ascii hyphen-split
common
```

```
# Create IPS as radius-server, which will be mapped in aaa profile. Enter the same
shared key as configured in IPS.
radius-server template rd-server-IPS
radius-server shared-key cipher %^%#~SZ#Wvmi~*}.Q`L'"|s;q9ci)(u&U4'!>:1Ja]T(%^%#
radius-server authentication <Radius-Server-IP> <1812> weight 80
radius-server accounting <Radius-Server-IP> <1813> weight 80
calling-station-id mac-format hyphen-split mode2 uppercase

# Configure the switch to support dynamic authorisation
radius-server authorization 192.168.10.11 shared-key cipher
%^%#qIj!'3LZN1TkF=JkGF:Gx:U$:!c]HES=$BG.*HwY%^%#
# Configure aaa profile
aaa
  authentication-scheme <auth-scheme>
    authentication-mode radius
  authorization-scheme default
  accounting-scheme <accounting>
    accounting-mode radius
    accounting realtime 15
  domain isp
    authentication-scheme <auth-scheme>
  accounting-scheme <accounting>
    radius-server <rad-server-IPS>

# Create VLAN interfaces which will be used for enforcement
# Endpoint will get IP address in the VLAN to which it is assigned.

interface Vlanif100
ip address 192.168.10.10 255.255.255.0
dhcp select interface

interface Vlanif200
ip address 192.168.20.10 255.255.255.0
dhcp select interface
# Access Interface having authentication-profile as dot1x
interface GigabitEthernet0/0/17
description "EP Interface"
port link-type hybrid
Port hybrid untagged vlan 100 200
authentication-profile <auth-profile-name>
# Interface Connected to IPS server
```

```
interface GigabitEthernet0/0/19
description "connected to IPS"
port link-type access
port default vlan 100
```

Configuration Commands: Juniper EX Series Switch

The below example shows a sample configuration of 802.1X authentication on Juniper EX switch.

The configuration involves the following:

- Configuring IPS server as a RADIUS server in edit mode.
- Configuring 802.1x on the switch port in edit mode.

Configuring IPS server as a RADIUS server

The sample configuration below shows how to add IPS server as a RADIUS authentication and accounting server on Juniper EX switch. You must execute the following commands in edit mode.

```
set access radius-server <RADIUS SERVER IP> secret <SHARED-KEY>
set access radius-server <RADIUS SERVER IP> source-address 10.204.88.30
--Execute this command for configuring RADIUS CoA
set access radius-server <RADIUS SERVER IP> dynamic-request-port 3799
--Execute this command to add IPS as a RADIUS server
set access profile 802.1X-access-profile authentication-order radius
set access profile 802.1X-access-profile accounting order radius
set access profile 802.1X-access-profile radius authentication-server <RADIUS SERVER
IP>
set access profile 802.1X-access-profile radius accounting-server <RADIUS SERVER IP>
```

Configuring 802.1x on the Switch Port

The below example shows a sample configuration of 802.1X / MAC address authentication on Juniper EX switch interface. You must execute the following commands in edit mode.

```
--Execute this command for 802.1X
set protocols dot1x authenticator authentication-profile-name 802.1X-access-profile
set protocols dot1x authenticator interface ge-0/0/0.0 supplicant multiple
--Execute this command for configuring MAC BYPASS
set protocols dot1x authenticator interface ge-0/0/0.0 mac-radius
--Execute this command for viewing the status of the session
Show dot1x interface ge-X/Y/Z detail
```

RADIUS Dictionary Files

This section contains dictionary translations for parsing requests and generating responses. All transactions are composed of Attribute/Value Pairs. The value of each attribute is specified as one of these valid data types shown in table.

Data	Description
hexadecimal	Hexadecimal string
hex1, hex4	1- or 4-byte hexadecimal number
string	0-254 octets (includes null terminator)
stringnz	0-254 octets (without null terminator)
ipv6addr	16 octets in network byte order (per RFC-3162)
ipv6prefix	2-18 octets in network byte order (per RFC-3162)
ipv6interface	8 octets in network byte order (per RFC-3162)
ipaddr	4 octets in network byte order
ipaddr-pool	IP address selected from an IP address pool
ipxaddr-pool	IPX network number selected from an IPX address pool
integer	32-bit value in big endian order (high byte first)
int1, int4	1- or 4-byte decimal number (integer is equivalent to int4)
time	32-bit value in big endian order; seconds since 00:00:00 GMT, Jan. 1, 1970

All attribute names and value names in the supplied radius.dct dictionary are derived from the RADIUS specification by replacing all nonalphanumeric characters with dashes (-).

The following dictionary format provides a mechanism for including secondary dictionaries from the text of a primary dictionary. For example, only the attribute/value definitions that differ from the RADIUS specification need to be listed in a primary dictionary for a vendor specific implementation. Definitions for the attribute/values that are common to both are brought in by including the radius.dct dictionary anywhere within the vendor dictionary.

The following rules apply to the creation and use of dictionaries:

- All comments begin with a pound sign (#) in column 0 OR appear on an attribute or value line with <white space>#<white space> as the Mandatory delimiter between dictionary data and comment text. (This is a simple parser.)
- Include another dictionary file with an at sign (@). The (@) character must be in column 0.
- All attribute and attribute value names and numeric codes must be unique within a single dictionary. Conflicts between dictionaries are resolved according to the following rules:
 - Attributes and values have precedence over any that are parsed later, and parsing is depth first.
 - For example, to override a baseline attribute, create a file with that attribute in it, followed by an include of the baseline file. Because the baseline file is parsed later than the desired override, the baseline file is ignored.
 - When two secondary dictionary definitions of an attribute or value conflict, the earlier include takes precedence.
 - Other than include files, there are two meaningful line entry formats in a dictionary -one for attributes and one for attribute values.
 - ATTRIBUTE_KEY ATTRIBUTE_NAME ATTRIBUTE_CODE DATA_TYPE FLAGS [COMMENT_DELIMITER COMMENT_TEXT]
 - VALUE_KEY ATTRIBUTE_NAME VALUE_NAME VALUE_CODE [COMMENT_DELIMITER COMMENT_TEXT]
- The legend for the last column of an attribute entry should be:
 - 'c' indicates a SINGLE value attribute that is a candidate for inclusion in a user's checklist.
 - 'C' indicates a MULTI value attribute that is a candidate for inclusion in a user's checklist.
 - 'r' indicates a SINGLE value attribute that is a candidate for inclusion in a user's reply list.
 - 'R' indicates a MULTI valued attribute that is a candidate for inclusion in a user's reply list.
 - 'o','O' ordered attribute, some attributes (such as Reply-Message) might need to be presented in a particular order to make sense.



- The absence of {C,c,R,r} flags indicates an item that is neither a reply nor a check list item (such as State, Proxy-State).
 - All FLAG characters on a given attribute line must be clustered together to parse properly. No white space is allowed between individual characters.
-

Policy Enforcement using MAC Authentication

Overview

Media Access Control (MAC) authentication is used to authenticate devices based on their physical MAC addresses. Using MAC authentication IPS accepts the device MAC address as user credentials, matches it with the local database or LDAP server and then assigns the port connecting the device to a predetermined VLAN. MAC addresses can be easily spoofed so we recommend you to create separate VLANs or filters specifically for devices using MAC authentication. For example, you can create separate a special VLAN or separate filters for each of the device type such as printers, VOIP phones, and so on. You can also use Profiler for device validation and MAC authentication. For more information, see Profiler.

MAC based authentication is not as secure as agent access or agentless access authentication. MAC addresses are not generally guarded as secrets, so an attacker can spoof a MAC address and impersonate a device to gain network access. To reduce risk of an exploit, create a special VLAN for each device type.

Benefits of MAC authentication

The benefits of MAC authentication are:

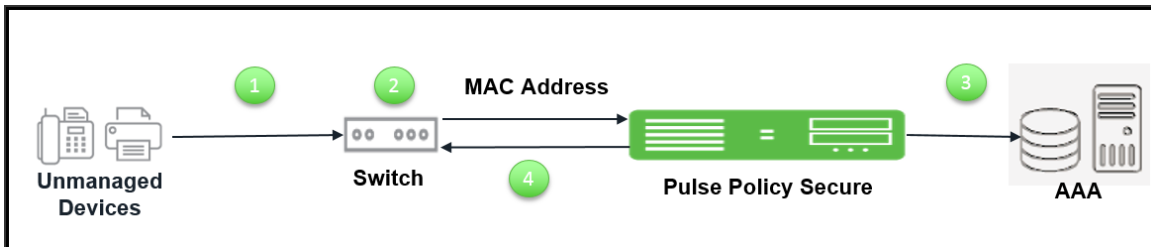
- IPS supports MAC authentication using both a local database and with LDAP servers.
- Supports authentication for unmanageable devices, such as printers, VOIP phones, and so on.
- Supports device validation and MAC authentication using Profiler.

Deployments using MAC Authentication

MAC address authentication is port-based security typically deployed at the edge of the network to enable secure access for devices, such as IP phones, printers, and network attached storage devices. The IPS MAC address authentication solution uses IPS 802.1x framework. When a device connects to a switch, the switch forwards the MAC address as the log in credential to IPS RADIUS server. Using MAC based authentication, the MAC address serves as both the username and the password. The RADIUS server consults the authentication server and sends back a RADIUS return attribute based on the authentication results.

Deployment of IPS using Local MAC Authentication Server

IPS supports MAC address authentication using a local Mac Authentication server. You can configure the IPS server to act as the authentication and policy server for MAC address authentication and optionally a separate directory/attribute server. You cannot use a RADIUS server with outer proxy authentication for MAC address authentication.

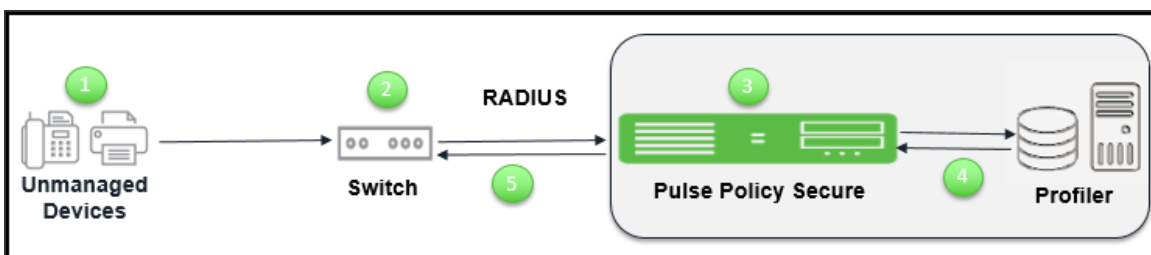


The authentication process is described below:

1. Unmanaged devices connect to network switch.
2. IPS accepts the device MAC address as username and password using MAC Authentication.
3. IPS matches the MAC address with the entries either in a local database or external database and then assigns a port connecting the device to a predetermined VLAN or filter id.
4. If the device MAC address is not found, then IPS places the device in a specified default VLAN.

Deployment of IPS using Profiler

IPS supports the device validation using Profiler. Profiler dynamically identifies and classifies endpoints across managed and unmanaged endpoint devices, so that access to network and resources can be controlled based on the type of the device.



The authentication process is described below:

1. Profiler discovers and classifies the endpoints on the network.
2. Unmanaged devices connect to network and the switch sends MAC RADIUS query.
3. IPS verifies the MAC address in Profiler database.
4. IPS then assigns role based on device attributes.
5. IPS assigns the switch port to appropriate VLAN or filter id.

For more information on Profiler, see *Ivanti Deployment Guide*.

Configuring MAC Authentication on IPS

To allow access for unmanageable devices, configure the necessary VLANs on your internal network to accommodate the different devices that you want to allow. On IPS, you assign devices to VLANs through the location groups that are added to RADIUS attributes policies.

Configuring the MAC Address Authentication Server

To support MAC authentication, add a MAC authentication server to IPS. You can either configure the MAC addresses directly on IPS or you can associate the MAC authentication server with an LDAP server.

To configure the MAC address authentication server:

1. Select **Authentication > Auth.Servers**.
2. Select **MAC Address Authentication** and click **New Server** to display the configuration page
MAC address authentication server configuration page.

Auth Servers > Demo-Mac-Auth-Server > Settings

Settings

Name: Demo-Mac-Auth-Server Label to reference this authentication.

MAC Addresses

Maximum 500 addresses

Delete [Up] [Down]

MAC Address	Action	Attributes	
<input type="text"/>	Allow	<input type="text"/>	Add
<input type="checkbox"/> 00:11:85:bb:8c:66	Allow	Session-Timeout=120;Termination-Action=1;demo-custom-attribute-mac-users=https://10.10.10.10	

Example MAC Address:
00:11:85:bb:8c:66
00:ff:****
Example Attribute:
attribute1=value1,attribute2=value2,
(for attribute: alphanumeric or "_" or "-" characters only)
The Allow & Attributes action accepts the defined MAC Address expression and looks it up in the optional LDAP Server(s) below for authorization attributes.

Optional LDAP Servers

Available LDAP Servers: (none) [Add ->] [Remove]

Selected LDAP Servers: (none) [Up] [Down]

To manage servers, see the [Server](#) configuration page.

Server Catalog


[Attributes...]

The attributes catalog should be used for both attributes defined in the MAC Addresses Table and the optional LDAP Servers.

[Save Changes] [Reset]

3. Complete the configuration as described in the below table.
4. Click **Save Changes** to save the configuration.

Settings	Guidelines
Name	Specify a name to identify the configuration. Follow a convention that is helpful to you and others who might perform administration tasks.
MAC Addresses	

Settings	Guidelines
MAC Address	Enter a MAC address. The system supports various formats, including no-delimiter (003048436665), single dash (003048-436665), multidash (00-30-48-43-66-65), and multicolon (00:30:48:43:66:65). The system supports wildcards (00:30:*:*:*:*). In the user log, entries appear in the multicolon format.
Action	Select an action to take when the MAC address matches: Allow -Signal successful authentication. Deny -Signal unsuccessful authentication. Allow and Attributes -Typically, a match terminates the search. If you select Allow and Attributes, the search is not terminated; instead, the system searches the LDAP servers for a match to retrieve the LDAP authorization attributes.
Attributes	Specify a name-value pair to associate the MAC address with a particular group or organization. For example, dept=eng is a name-value pair that associates the MAC address with a department (engineering). When you create the MAC address realm, you can create a custom expression to assign the MAC address to a specific role. Radius Return Attributes from the dictionaries is pre-populated to the Server Catalog of MAC Auth server so that they are available under the custom attributes for a specific user.
Optional LDAP Servers	
Available / Selected LDAP Servers	Use the Add and Remove selector buttons to add LDAP servers to the list of selected servers. Use the up and down buttons to order the list. The order in which the LDAP servers are listed is important. The system searches for MAC address matches in the following order: If the MAC address of the endpoint matches a manual entry, the system does not query servers in the LDAP server list. If no manual entries match, the system tries the first LDAP server. If the request times out or gets rejected, the system tries the second, then the third, and so on. <hr/>  Each LDAP server that must be queried affects performance. <hr/>
Server Catalog	

Settings	Guidelines
Attributes	If you have selected LDAP servers in the configuration, save the configuration. After you have saved the configuration, the Attributes button is displayed. Click the Attributes button to display the LDAP server catalog, which you can use to select or add attributes to be retrieved from the LDAP servers.

Configuring the MAC Address Authentication Realm and Role Mapping Rules

The MAC address authentication framework uses a special realm called the MAC Address Authentication Realm. You need not configure a sign-in policy while using MAC address authentication realm. The MAC Address authentication realm uses any username credential that matches one of the common variants of a MAC address format (colon-separated, dash-separated, and the like) and sends it to the MAC authentication realm based on its format.

To configure the MAC Address authentication realm and role mapping rules:

1. Select **Endpoint Policy > MAC Address Realm**.
2. Click **New** to create a new configuration.

MAC Address Realms > New Authentication Realm

New Authentication Realm

Name:

Description:

When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication:

User Directory/Attribute:

Accounting:

Device Attributes:

Dynamic policy evaluation

Enable dynamic policy evaluation

[Save Changes](#)

3. Complete the configuration. The following table summarizes the key settings.

Setting	Guideline
Name	Enter the name of the realm.
Description	Enter the description for identifying the realm.
Server	
Authentication server	Select the MAC Address authentication server configured.
User Directory/Attribute	Select the LDAP authentication server configured.
Accounting	Select the MAC Address authentication server configured.
Device attribute	Specify the server for device authorization. For profiler, select the name of the local profiler.
Dynamic Policy Evaluation	
Dynamic Policy Evaluation	Select this option to automatically or manually refresh the assigned roles of users by evaluating a realm's authentication policy, role-mappings, role restrictions, and resource policies.

4. Save the configuration. Upon saving the new realm, the system displays the role mapping rules page. Under Role Mapping tab, click **New Rule**. Role Mapping Rule page appears.
5. Select **Device Attribute** under **Rule based on** tab and click **Update**. Enter the name for the rule.
6. Select the relevant Attribute under Attributes tab for Role Mapping and enter an appropriate value.
7. Select an appropriate role from Available Roles and Click **Add** to Selected Roles.

- Click **Save Changes** to save the configuration settings.

The screenshot shows the 'Role Mapping Rule' configuration page. At the top, the breadcrumb is 'MAC Address Realms > MAC_Realm > Role Mapping > Role Mapping Rule'. The page title is 'Role Mapping Rule'. Below the title, there is a 'Rule based on:' dropdown set to 'Username' and an 'Update' button. A required field '* Name:' is present. A section titled 'Rule:if username...' contains a dropdown set to 'is' and a text input field. A note states: 'If more than one username should match, enter one username per line. You can use * wildcards.' Below this is a section 'then assign these roles' with two columns: 'Available Roles' and 'Selected Roles'. The 'Available Roles' list includes Guest, Guest Admin, OnboardRole, remed, and Users. The 'Selected Roles' list is currently empty, showing '(none)'. There are 'Add ->' and 'Remove' buttons between the columns. At the bottom, there is a checkbox 'Stop processing rules when this rule matches' and a note 'To manage roles, see the Roles configuration page.' Two buttons, 'Save Changes' and 'Save + New', are at the bottom. A small note '* indicates required field' is at the very bottom.

Configuring User Roles for the MAC Address Authentication Realm

IPS access management framework evaluates authentication requests to match endpoints to roles. You must configure user roles for the various types of endpoints authenticated by the MAC address authentication framework.

To create a user role:

- Select **Users > User Roles**.
- Click **New Role**.
- Complete the name and description configuration and then save the configuration.

- Click **Agent** and deselect agent options and then save the configuration.

The screenshot shows the 'New Role' configuration page. At the top, it says 'User Roles > New Role'. Below that, there's a 'New Role' section with a 'Name:' label and an empty text input field, and a 'Description:' label with a larger empty text area. Underneath is an 'Options' section with a dropdown arrow. A note states: 'Session and appearance options are specified in Default Options. Check the following if this role should override these defaults.' There are five checkboxes: 'Session Options' (checked), 'UI Options' (checked), 'Odyssey Settings for Access' (unchecked), 'Odyssey Settings for Preconfigured Installer' (unchecked), and 'Enable Guest User Account Management Rights' (unchecked). At the bottom left is a blue 'Save Changes' button.

- Click Agentless and enable agentless access and then save the configuration.

The screenshot shows the 'Agent' configuration page. At the top, it says 'User Roles > Users > Agent > General'. Below that, there's a 'General' section with three tabs: 'General', 'Agent' (selected), and 'Agentless'. Underneath the tabs, there's a 'General' sub-tab and an 'Odyssey Settings' sub-tab. Below that is an 'Options' section with a dropdown arrow. There are two checkboxes: 'Install Agent for this role' (unchecked) and 'Enable Host Enforcer' (unchecked). A note for 'Enable Host Enforcer' says: 'Note:(Odyssey Access Client only) By default, if you enable Host Enforcer on a role, all traffic is blocked for users mapped to this role. Make sure you create Host Enforcer policies on the "Resource Policies>Host Enforcer" page to allow particular traffic for this role. Host Enforcer policies that apply to this role: Access control'. Below that is a 'Session scripts' section with two columns: 'Windows: Session start script' and 'Windows: Session end script'. Each column has a description and a 'Script Location:' label with an empty text input field. At the bottom left is a blue 'Save Changes' button.



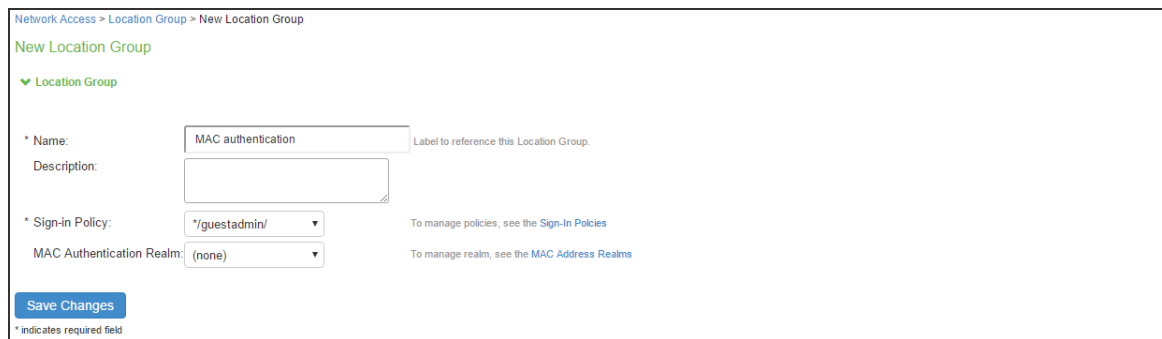
Do not configure role restrictions for roles used with a MAC address authentication realm.

Configuring a Location Group

Location groups let you organize or logically group network access devices by associating the devices with specific sign-in policies. Sign-in policies provide a way to define and direct independent access control policies with the network. For example, you can create location group policies to logically group the network access devices in each building at a corporate campus. You can also use location group policies to specify a special realm for MAC address authentication.

To configure a location group:

1. Create a sign-in policy to associate with the location group.
2. Select **Endpoint Policy > Network Access > Location Group**.



The screenshot shows the 'New Location Group' configuration page. The breadcrumb trail is 'Network Access > Location Group > New Location Group'. The page title is 'New Location Group'. Under the 'Location Group' section, there are four fields: 'Name' (text input with 'MAC authentication' entered), 'Description' (text area), 'Sign-in Policy' (dropdown menu with '/guestadmin/' selected), and 'MAC Authentication Realm' (dropdown menu with '(none)' selected). There are two links: 'Label to reference this Location Group.' next to the Name field, and 'To manage policies, see the Sign-In Policies' and 'To manage realm, see the MAC Address Realms' next to the Sign-in Policy and MAC Authentication Realm fields respectively. A 'Save Changes' button is at the bottom left. A note at the bottom left states '* indicates required field'.

3. On the New Location Group page, enter a name to label this location group and optionally a Description.
4. For Sign-in Policy, select the sign-in policy associate with the location group.
5. For controlling an unmanageable device using MAC address authentication, select a MAC Authentication Realm that you created from the list.
6. Click **Save Changes**.

Configuring RADIUS Client

A RADIUS client policy specifies the information required for unmanaged devices to connect as a RADIUS client of the IPS.

To configure a RADIUS client:

1. Select **Endpoint Policy > Network Access > RADIUS Client**.
2. Click **New RADIUS Client**.

▼ RADIUS Client

🟢 Cisco WLC 10.204.88.244 successfully updated. ✕

* Name: Label to reference this RADIUS Client.

Description:

* IP Address: IP Address of this RADIUS Client.

* IP Address Range: Number of IP Addresses for this RADIUS Client

* Shared Secret: RADIUS shared secret

Key Wrap Key Wrap (Support for RFC 6218)

* Key Wrap Format: Key Wrap Format

* Key Encryption Key(KEK): Key Encryption Key(KEK), size should be 16 bytes

* Message Authentication Code Key(MACK): Message Authentication Code key (MACK), size should be 16 bytes to 64 bytes

* Make/Model: To manage make/model, see the [RADIUS Vendor](#)

* Location Group: To manage groups, see the [Location Group](#)

▼ Dynamic Authorization Support

Support Disconnect Messages Disconnect Message Support

3. On the RADIUS Client page, enter a name to label the RADIUS client. You can assign any name to a RADIUS client entry, use the device's SSID or IPv4 address to avoid confusion.
4. Enter a purpose or description of the configuration so that other users are aware of it.
5. Enter the IP address of the NAD.
6. (Optional) For **IP Address Range**, enter the number of IP addresses in the IP address range for the switch/WLC, starting with the address you specified for IP Address. You can specify a range up to a maximum of 32,768 addresses.
7. For **Shared Secret**, enter the RADIUS shared secret. A RADIUS shared secret is a case-sensitive password used to validate communications between IPS and NAD. IPS supports shared secrets of up to 127 alphanumeric characters, including spaces and the following special characters:
~!@#\$%^&*()_+|\=-'{}[]:";<>?/.,
8. For **Make/Model**, select the make and model of the NAD. The make/model selection tells IPS which dictionary of RADIUS attributes to use when communicating with this client.
9. For **Location Group**, select the location group to use with this NAD.

10. Under **Dynamic Authorization support**, Select the **Support Disconnect Messages** check box to send disconnect messages to supplicants if access is no longer authorized. If this check box is selected, a disconnect request is sent to the NAD any time a session is deleted. IPS can also send disconnect messages upon a role event that includes a VLAN change or a change in RADIUS attributes.
11. Select **Support CoA Messages** to enable CoA messages and disconnect messages support for the client.
12. (Optional) Enter a new **Dynamic Authorization Port** (Default port is 3799). The default port might vary depending on the manufacturer. NAD listens to UDP port to receive RADIUS CoA messages from IPS.
13. Click **Save Changes**.



MAC address authentication must be enabled on the switch port. See [Configuring 802.1x and MAC Authentication](#) on the Switch Port for switch configuration.

Configuring RADIUS Attributes

This configuration describes the configuration information for RADIUS return attributes policy that is applied on switch, request attribute policy, which can be used along with sign-in policies for realm selection, policy realm restrictions, and authentication/accounting reporting for RADIUS authentication events.

This configuration describes how to send VLAN assignment and other attributes to the switch/WLC by returning RADIUS attributes.

1. Select **PPS > Network Access > RADIUS Attributes**, and then select VLAN.
2. Specify a VLAN ID.
3. Select Return Attribute.
4. Select the attribute you want to return from the Attribute list.
5. For Value, specify an attribute value.

IP Address Pools

In current implementation, the IPS supports only static IP address assignment. From 9.1R13, IPS also allows the admins to assign IP addresses dynamically for the users or nodes from IP address pools.

When the RADIUS authentication succeeds, if the pool name is configured in the Framed-IP-Address return attribute, then the available IP address is assigned to the user from the corresponding IP address pool. When the user session ends (on receiving acct-stop or admin deletes the user session), the assigned IP address is released back to the pool.

In order to release the IP address when a user is deleted from the active user page, it is necessary to have received an "accounting start" request after authentication request by the user/node.



IP address pools are not supported for Pulse dot1x and native dot1x use cases.

Configuring IP Address Pool

To configure the IP address pools, use the following procedure:

1. Navigate to **Endpoint Policy > Network Access > IP Address Pools**. The page lists the existing IP address pools. Click **New IP Address Pool...** to add a new address pool.

The screenshot shows the 'IP Address Pools' configuration page. At the top, there are several tabs: RADIUS Dictionary, RADIUS Vendor, Location Group, RADIUS Client, IP Address Pools (selected), RADIUS Attributes, Network Infrastructure Device, and SNMP Enforcement Policies. Below the tabs, there is a text box explaining that the RADIUS return attribute 'Framed IP address' specifies the IP address pool name. There are two buttons: 'New IP Address Pool...' and 'Delete'. Below this, there is a dropdown menu set to '10 records per page' and a search box. A table with two columns, 'Name' and 'Description', is shown. The table contains one entry: 'Pool1'. At the bottom right of the table, there are navigation buttons: 'Previous', '1', and 'Next'.

2. Add the name and IP address range for the IP address pool and save the changes.

Network Access > IP Address Pools > New IP Address Pool

New IP Address Pool

* Name:

Description:

Address Ranges

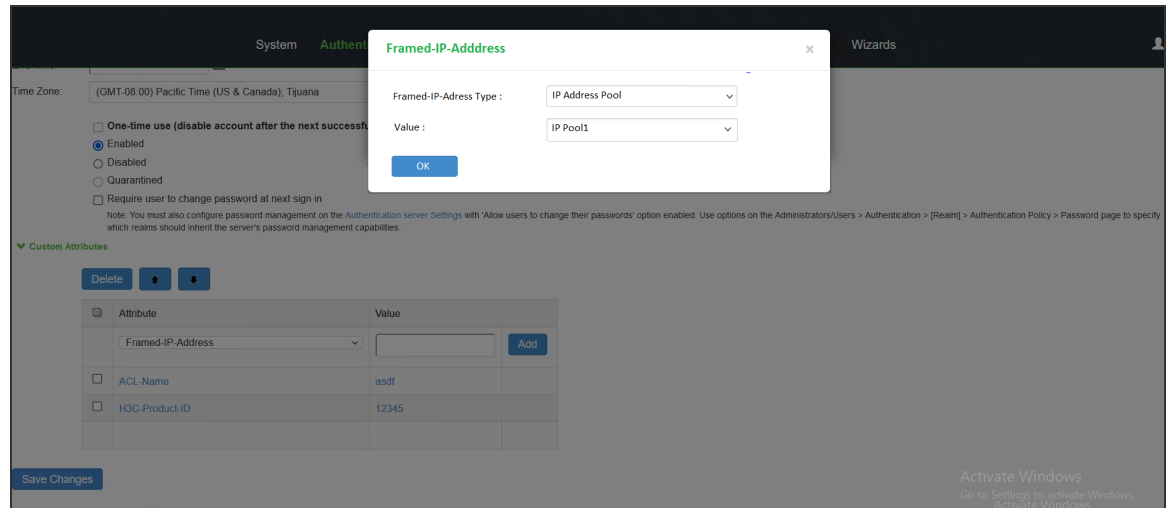
Delete

	Starting IP Address	Range	
	<input type="text"/>	<input type="text"/>	Add

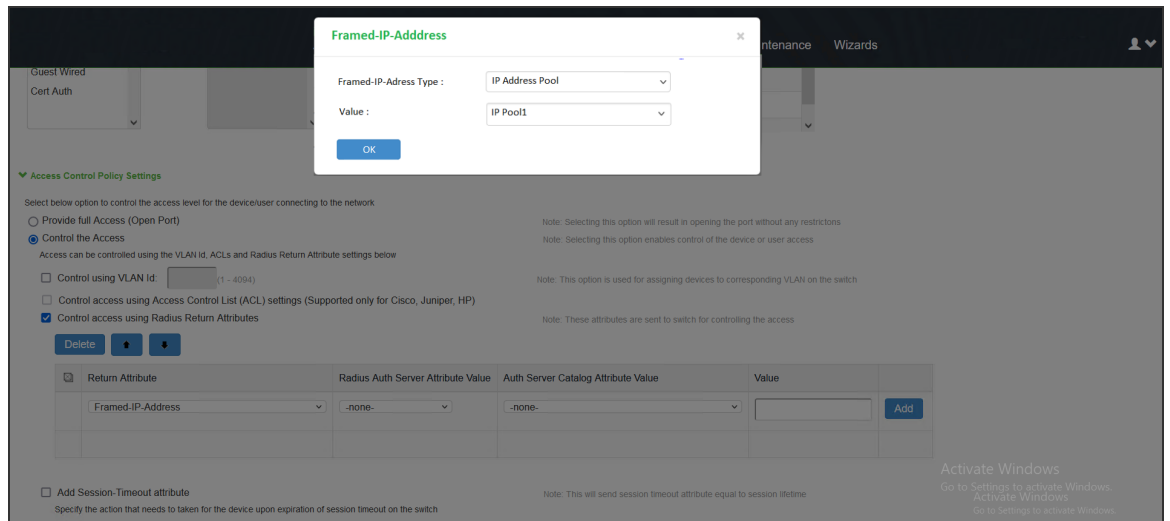
Save Changes

* indicates required field

3.
 1. To configure IP address pools for System Local Users, use the following procedure:
 - For System Local Users, under **Custom Attributes**, select **Framed-IP-Address**. Then select **IP Address Pool** as the type and select the name of the IP address pool to add to the attribute list.



- (Mandatory) If Radius Return Attributes policy is configured, then under **Access Control Policy Settings** do one of the following:
 - Map the **Framed-IP-Address** attribute to the auth server catalog attribute.
 - Select **Framed-IP-Address**. Then select **IP Address Pool** as the type and select the name of the IP address pool to add to the attribute list.



4. To configure IP address pools associated with Radius Client, use the following procedure:

- For Radius Clients, select the IP address pool from the list.

- Once Radius client is associated with the IP pool configuration, associate it with Framed-IP-Address attribute in Radius Return Attribute Policy or User catalog attributes.

Attribute	Value
Framed-IP-Address	
ACL-Name	asdf
H3C-Product-ID	12345



The user catalog attribute value takes precedence over the value associated with Radius Return Attribute policy.

Delegated Admin Control

This feature allows super admin to configure different access levels to RADIUS, SNMP policies and RADIUS Clients, SNMP Clients configurations listed under Endpoint Policy → Network Access.

A super admin can configure a delegated admin role and assign permission levels (Read/Write/Deny) for Network Access Clients and Network Access policies in the Delegated Admin role configuration.

On successful login to IPS, the delegated admin is assigned the permissions as set by super admin.

Admin Roles > test_read > Resource Policies

Resource Policies

General System Users Administrators **Resource Policies**

Specify the delegated admin role's level of access to various resource policies. You may set access levels (read, write, deny) for all resource policies or you may set custom access levels per policy type or individual policy (Additional Access Policies). The Write access for the Additional Access Policies will only allow the admin to change the assigned user roles and the detailed rules in the policy.

▼ Delegate resource policies

Deny All

	Deny	Read	Write	
Infranet Enforcer:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	▶ 0 Additional Access Policies
Host Enforcer:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	▶ 0 Additional Access Policies
Specify level of access to RADIUS Dictionary, RADIUS Vendor, Location Group, RADIUS Client, Network Infrastructure Device using Network Access Clients option. Specify level of access to RADIUS Attributes, SNMP Enforcement Policies using Network Access Policies option.				
Network Access Clients:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	▶ 0 Additional Access Policies
Network Access Policies:	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	▶ 0 Additional Access Policies

[Save Changes](#)

Policy Enforcement using SNMP/SSH

Overview

IPS supports device visibility and policy enforcement on switches using SNMP as an alternative to 802.1X. Using SNMP enforcement, you can easily deploy and achieve comprehensive compliance and role based access.

Benefits of SNMP Enforcement

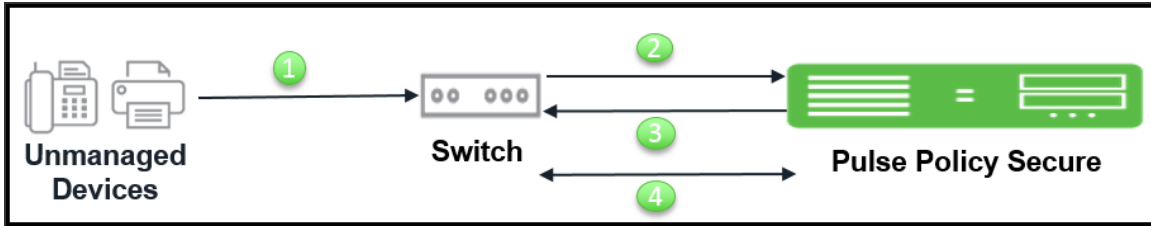
The following are the benefits of SNMP enforcement:

- Supports SNMP enforcement for MAC based authentication and role assignment.
- Supports network visibility using SNMP v1/v2/v3.
- The endpoints are discovered through SNMP traps (Linkup/Down, MAC notification, and Port security).
- Supports easy NAC deployment with SNMP enforcement based on compliance and role-based access.
- Supports Non-802.1X compliance endpoints.
- Supports SNMP discovery for L2/L3 switches.
- Supports Pulse session after SNMP MAC authentication.
- Supports hybrid deployment- 802.1X for wireless network and SNMP for wired network.

Policy Enforcement Using Simple Network Management Protocol/SSH

Policy Enforcement using SNMP for Unmanaged Devices

To deploy policy enforcement using SNMP for unmanaged devices, add the switch as an SNMP Agent and the IPS device as an SNMP server in the switch and then configure the SNMP Enforcement Policies in IPS.



The workflow for the SNMP policy enforcement using *linkup/MAC address Notification traps* is described below:

1. Unmanaged corporate devices such as phones, printers, and cameras connect to SNMP switch. The SNMP switch is configured for linkup/MAC address Notification trap. The SNMP switch generates the SNMP trap. See the Appendix section for switch configuration.
2. IPS learns or receives the MAC address.
3. IPS performs the MAC authentication and sets the VLAN/ACL based on the role assigned using SNMP.
4. When the user disconnects the device from the switch by plugging out the cable, IPS receives an SNMP trap and it deletes the session from the IPS server and sets the switch port to the default VLAN/ACL.

The workflow for the SNMP policy enforcement using *port-security trap* is described below:

1. Unmanaged corporate devices such as phones, printers, and cameras connect to SNMP switch. The SNMP switch is configured for port-security trap. A dummy static MAC address is configured on the port. Since machine's MAC address does not match with the configured dummy mac address, it generates a security violation and a port security trap is sent to IPS. See the Appendix section for switch configuration.
2. IPS learns or receives the MAC address.
3. IPS performs the MAC authentication and the dummy MAC address configured on the interface is replaced with the endpoint MAC address thus authorizing the endpoint on the switch and sets the VLAN based on the role assigned.
4. When the user disconnects the device from the switch by plugging out the cable, the session is not deleted from the IPS. However, the session is deleted only after the session timeout.

Policy Enforcement using SNMP for Managed Devices

To deploy policy enforcement using SNMP for managed devices, add the switch as an SNMP Agent and the IPS device as an SNMP server in the switch and then configure the SNMP Enforcement Policies in IPS.



The workflow for the SNMP policy enforcement using *link-up/MAC address Notification traps* is described below:

1. Managed corporate client (Pulse Desktop client is installed) such as Windows/MAC OSX machine connects to SNMP switch port. The SNMP switch is configured for link-up/MAC address Notification trap. The SNMP switch generates the SNMP trap. See Appendix section for switch configuration.
2. IPS learns or receives the MAC address.
3. IPS performs the MAC authentication and sets the VLAN/ACL based on the role assigned using SNMP.
4. The user connects to IPS using Pulse Client. Host checker evaluates the compliance status of machine. If machine is compliant with Host Checker policy.
5. IPS sets the VLAN/ACL configured for compliant role using SNMP and if machine is non-compliant with Host Checker policy then IPS sets the VLAN/ACL configured for non-compliant role using SNMP.
6. When the user disconnects the Pulse client. IPS reevaluates the role and sets the VLAN/ACL based on the role assigned.
7. When the user disconnects the endpoint from the switch by plugging out the cable, session from the IPS server is deleted and the switch port is set to the default VLAN/ACL.

The workflow for the SNMP policy enforcement using *port-security trap* is described below:

1. Managed corporate client (Pulse Desktop client is installed) such as Windows/MAC OSX machine connects to SNMP switch port.
The SNMP switch need to be configured for port-security trap. A dummy static MAC address is configured on the port. Since the machine's MAC address does not match with the configured dummy mac address, it generates a security violation and a port security trap is sent to IPS.
2. IPS learns or receives the MAC address.
3. IPS performs the MAC authentication and the dummy MAC address configured on the interface is replaced with the endpoint MAC address thus authorizing the endpoint on the switch and sets the VLAN based on the role assigned.
4. When the user disconnects the device from the switch by plugging out cable, the session is not deleted from the IPS. However, the session is deleted only after the session timeout.
5. IPS sets the VLAN configured for compliant role using SNMP and if machine is non-compliant with Host Checker policy then IPS sets the VLAN configured for non-compliant role using SNMP.
6. When the user disconnects the Pulse client. IPS reevaluates the role and sets the VLAN based on the role assigned.
7. When the user disconnects the device from the switch by plugging out the cable, the session is not deleted from the IPS. However, the session is deleted only after the session timeout.

-
- If the SNMP switch supports MAC Notification traps (MAC added notification trap), you must enable the traps in addition to the Link Up / Link Down traps.
 - If Port Security traps are enabled, LinkUp/LinkDown or MAC Added Notification traps should not be enabled.



- IPS does not support MAC removed notifications trap. It tracks the session / MAC address associated with a particular interface and removes it once a link down trap is received.
 - MAC notification traps are supported only for Cisco and HP switches.
 - SNMP Enforcement using ACL is not supported using Port-Security traps.
-

Configuring SNMP Policy Enforcement using VLAN (Cisco, HP)

This section covers the configuration for SNMP policy enforcement. SNMP based policy enforcement is applied to endpoints running Pulse Client, and to clientless endpoints where the MAC address is discovered through SNMP. For endpoints running Pulse Client, role assignment is based on compliance; for clientless endpoints, role assignment is based on MAC address.

Configuring a MAC address Authentication Server

A MAC address authentication server defines how endpoints are authorized using the MAC address. You can choose to allow or deny a MAC address or use wildcards to allow or deny groups of MAC addresses.

To configure a MAC address authentication server:

1. Select **Authentication > Auth Server**.
2. Select **MAC Address Authentication** and click **New Server** to display the MAC Address Authentication Server configuration page as shown in figure.

The screenshot shows the configuration page for a MAC Address Authentication Server named 'MACAuthServer'. The page is divided into several sections:

- Name:** MACAuthServer (Label to reference this authentication.)
- MAC Addresses:** A table with columns for MAC Address, Action, and Attributes. The table contains one entry with a wildcard MAC address and an 'Allow' action. A 'Delete' button and a '+ Add' button are visible. A note indicates a maximum of 500 addresses.
- Optional LDAP Servers:** Two boxes labeled 'Available LDAP Servers' and 'Selected LDAP Servers', both currently containing '(none)'. 'Add ->' and 'Remove' buttons are between them.
- Server Catalog:** An 'Attributes...' button with a note: 'The attributes catalog should be used for both attributes defined in the MAC Addresses Table and the optional LDAP Servers.'
- Buttons:** 'Save Changes' and 'Reset' buttons at the bottom.

Example MAC Address: 00:11:85:5b:8c:66
00:ff:ff:ff:ff:ff
Example Attribute: attribute1=value1;attribute2=value2;
(for attribute: alphanumeric or '-' or '_' characters only)
The Allow & Attributes action accepts the defined MAC Address expression and looks it up in the optional LDAP Server(s) below for authorization attributes.

3. On the MAC address authentication server configuration page:
 - For Name, enter a name to label this MAC address authentication server.
 - Under MAC Addresses, enter the MAC address(es) to whitelist.
 - Select an action to take when the MAC address matches:
 - **Allow**-Signal successful authentication.
 - **Deny**-Signal unsuccessful authentication.
 - **Allow and Attributes**-Typically, a match terminates the search. If you select Allow and Attributes, the search is not terminated; instead, the system searches the LDAP servers for a match in order to retrieve the LDAP authorization attributes.
 - Specify a name-value pair to associate the MAC address with a particular group or organization.
 - Under Optional LDAP servers, Use the **Add** and **Remove** selector buttons to add LDAP servers to the list of selected servers. Use the up and down buttons to order the list. The order in which the LDAP servers are listed is important.
 - Under Server Catalog, Click the **Attributes** button to display the LDAP server catalog, which you can use to select or add attributes to be retrieved from the LDAP servers.
4. Click **Save Changes** to save the configuration.

Configuring a MAC address Authentication Realm and Role Mapping

A MAC address authentication realm uses a MAC address authentication server and role mapping rules to sort MAC address authentication requests into roles.

To configure a MAC address authentication realm:

1. Select **Endpoint Policy > MAC Address Realms**.
2. Click **New** to display the MAC Address Realm configuration page.

3. On the MAC address realm configuration page:
 - For Name, enter a name to label this MAC address realm.
 - (Optional) For description, enter a description.
 - For Authentication Server, select the MAC address authentication server configured earlier.
 - For User Directory/Attribute Server, select "Same as above".
 - For accounting, select the authentication server.
 - For device attribute, select the server for device authorization. For profiler, select the name of the local profiler.
 - Specify the device check interval in minutes.
 - Select the **Enable dynamic policy evaluation** to automatically or manually refresh the assigned roles of users by evaluating a realm's authentication policy, role-mappings, role restrictions, and resource policies.
4. Click **Save Changes** to save the configuration.

Role mapping rules define how endpoints are assigned to roles.

To configure the role mapping rules for your MAC Address Realm:

1. Click the **Role Mapping** tab to display the role mapping configuration page for the realm.
2. Click **New** to display the MAC Address Realm configuration page.
3. On the role mapping configuration page, click **New Rule** to display the role mapping rule configuration page.

- (Optional) For Name, enter a name to label this role mapping rule.
 - Select the rule from the Rule based list and provide the appropriate details.
 - Select the appropriate role and click **Add**.
4. Click **Save Changes** to save the configuration.

Configuring a Location Group

A location group enables association of a sign-in policy and MAC address realm for network access policy enforcement.

To configure a location group:

1. Select **Endpoint Policy > Network Access > Location Group**.
2. Click **New Location Group** to display the Location Group configuration page.

Network Access > Location Group > New Location Group

New Location Group

▼ Location Group

* Name: Label to reference this Location Group.

Description:

* Sign-in Policy: To manage policies, see the [Sign-In Policies](#)

MAC Authentication Realm: To manage realm, see the [MAC Address Realms](#)

[Save Changes](#)

* indicates required field

3. On the location group configuration page:
 - Enter a name or label to describe the location group.
 - Enter a description.
 - Select the default sign-in policy as it is not applicable for SNMP enforcement. For example, default */ sign-in policy.
 - Select the MAC authentication realm which was configured earlier.
4. Click **Save Changes** to save the configuration.

Configuring SNMP Devices

You can add an SNMP device manually through SNMP device configuration or automatically discover SNMP devices through SNMP Device Discovery configuration.

Manual Addition of SNMP Devices

You can manually add SNMP devices from IPS. This section describes the SNMP device configuration for switches with different versions.

- Configuring devices with SNMP v1/v2c
- Configuring devices with SNMP v3

Configuring Devices with SNMP v1/v2c

To configure the device with SNMP v1/v2c:

1. Select **Endpoint Policy > Network Access > Network Infrastructure Device** and click **New Network** Infrastructure Device.
2. Enter a name to label this SNMP device.
3. For Description, enter a description. (Optional)
4. Enter the IP address of the SNMP device. You must enter a single IP address, not an IP address range or subnet.
5. Select the device vendor. SNMP VLAN enforcement check box will appear only for vendors who support SNMP enforcement. VLAN enforcement is supported only for HP and Cisco switches.
6. Under Enforcement, enable the **VLAN Enforcement** checkbox for using the device for SNMP enforcement using VLAN.
For Profiler, you must disable SNMP enforcement; the **Location Group, Default VLAN, Write Community** and **Trap Community String** fields are not applicable for profiling. A device so added is not used for enforcement.
 - For Location Group, select the location group configured earlier. Only location groups which have MAC Address Realms associated will be available for selection.
 - For Default VLAN, enter the VLAN to be provisioned when the SNMP user session is deleted or no endpoint is connected.
7. Under SNMP Settings, select **SNMP version v1/v2c**.
8. To use different credentials for write and trap community strings, disable the "Use same credentials for write and trap operations" check box.
9. Enter the community string(s) for the Read community.

- Click **Save Changes** to save the configuration.

Network Access > Network Infrastructure Device > New Network Infrastructure Device

New Network Infrastructure Device

*Name: Label to reference this Device.

Description:

*IP Address: IP Address of this Device.

*Vendor: Device Vendor.

Enforcement

ACL and/or VLAN will be used as an enforcement attribute to provision the policy for the endpoint. VLAN Enforcement is supported only for HP and Cisco.

Enforcement is supported only for Wired Switches.

ACL Enforcement VLAN Enforcement

*Location Group: Only groups which are associated with a MAC Address realm appear here. To manage groups, see the [Location Group](#)

*Default VLAN: To set the device interface to default VLAN specified value when there is no ROLE assigned. This is mainly used when a SNMP session is deleted.

SNMP Settings

*SNMP Version: v1/v2c v3

Same credentials for Write and Trap user

*Read Community String:

Configuring Devices with SNMP v3

To configure the switch with SNMP v3:

- Select **Endpoint Policy > Network Access > Network Infrastructure Device**.
- Click **New Infrastructure Device**.
- Enter a name to label this SNMP device.
- For Description, enter a description. (Optional)
- Enter the IP address of the SNMP device. You must enter a single IP address, not an IP address range or subnet.
- Select the device vendor. SNMP VLAN enforcement check box will appear only for vendors who support SNMP enforcement. VLAN enforcement is supported only for HP and Cisco switches.

7. Under Enforcement, enable the **VLAN Enforcement** checkbox for using the device for SNMP enforcement using VLAN.
For Profiler, you must disable SNMP enforcement; the **Location Group, Default VLAN, Write Community and Trap Community String** fields are not applicable for profiling. A device so added is not used for enforcement.
 - For Location Group, select the location group configured earlier. Only location groups which have MAC Address Realms associated will be available for selection.
 - For Default VLAN, enter the VLAN to be provisioned when the SNMP user session is deleted or no endpoint is connected.
8. Under SNMP Settings, select **SNMP version v3** and define the SNMP switch settings:
9. Enter the Read Username, select the Read Security Level and Auth Protocol, and enter the Auth Password.
10. To use different credentials for write and trap community strings, disable the "Use same credentials for write and trap operations" check box.
11. Click **Save Changes** to save the configuration.

Network Access > Network Infrastructure Device > New Network Infrastructure Device

New Network Infrastructure Device

*Name: Label to reference this Device.

Description:

*IP Address: IP Address of this Device.

*Vendor: Device Vendor.

Enforcement

ACL and/or VLAN will be used as an enforcement attribute to provision the policy for the endpoint. VLAN Enforcement is supported only for HP and Cisco.

Enforcement is supported only for Wired Switches.

ACL Enforcement VLAN Enforcement

*Location Group: Only groups which are associated with a MAC Address realm appear here. To manage groups, see the [Location Group](#)

*Default VLAN: To set the device interface to default VLAN specified value when there is no ROLE assigned. This is mainly used when a SNMP session is deleted.

SNMP Settings

*SNMP Version: v1/v2c v3

Same credentials for Write and Trap user

*Read Username:

*Read Security Level:

*Auth Protocol:

*Auth Password: Minimum 8 characters.



If you unplug a cable from an interface, the associated session would be deleted only if link down traps are enabled. If the port security traps are configured on the device, unplugging of the cable does not cause session deletion.

Auto Discovery of SNMP Devices

IPS provides an optional SNMP Device Discovery option. You can specify a range of IP addresses and other details needed for SNMP configuration to perform discovery of SNMP enabled devices.

IPS discovers all SNMP enabled L2 or L3 devices. SNMP enabled devices, which are not supported are listed as unsupported and cannot be added to the SNMP devices page.

To discover SNMP enabled devices:

1. Select **Endpoint Policy > Network Access > Network Infrastructure Device > Discovery**.

The screenshot shows the 'SNMP Device Discovery' configuration page. At the top, there are tabs for 'RADIUS Dictionary', 'RADIUS Vendor', 'Location Group', 'RADIUS Client', 'RADIUS Attributes', 'SNMP Device' (selected), and 'SNMP Enforcement Policies'. Below the tabs, there is a 'Configuration' section with a 'Discovery' sub-tab. A note states: 'Atleast one of v2 or v3 settings need to be configured for enabling SNMP Discovery.' The configuration includes:

- *IP address/range: 10.204.88.16 (with a note: IP address or range of IP addresses in CIDR format)
- SNMP V2 Settings: * Community string: Prof
- SNMP V3 Settings: *User name: (empty), Authentication protocol: MD5, Authentication Password: (empty), Privacy protocol: CBC-DES, Privacy Password: (empty)

 A 'Discover' button is present. Below it is a table with the following data:

Name	IP Address	SNMP Version	Device Details	SNMP Enforcement	Location Group	Default Vlan
1	10.204.88.16	V2	Vendor: CISCO Name: Profiler3750 Descr: Cisco IOS Software, C3750 Software (C3750-IPSERV) Location: Bangalore	<input checked="" type="checkbox"/>	initialSetup_snmp	123

 An 'Add Device' button is located at the bottom left of the table area.

2. On the SNMP device discovery configuration page:

- For IP Address Range, enter a range of IP addresses in CIDR format (for example, 10.204.88.0/28) to discover SNMP devices.
- To discover SNMP v1/v2c devices, enter the community string to use with SNMP v1/v2c device.
- To discover SNMP v3 devices, enter the user name to use with SNMP v3 devices. Enter the Authentication protocol, Authentication password, Privacy protocol and Privacy password for SNMP v3 devices.
- Click **Discover** to start the discovery process.

Once the devices are discovered, you must complete the following configuration for SNMP enforcement on each device:

1. Choose a location group from the dropdown list.
2. You can enable the SNMP VLAN enforcement for the supported switches (HP/Cisco).
3. Specify a default VLAN.
4. Select the devices to be added and click **Add Device**.
5. Click **Save Changes**.

The SNMP enforcement option is disabled for the Switches, which don't support SNMP enforcement.

Network Access > SNMP Device Discovery > SNMP Device Discovery

SNMP Device Discovery

RADIUS Dictionary | RADIUS Vendor | Location Group | RADIUS Client | RADIUS Attributes | **SNMP Device** | SNMP Enforcement Policies

Configuration | **Discovery**

Atleast one of v2 or v3 settings need to be configured for enabling SNMP Discovery.

*IP address/range: IP address or range of IP addresses in CIDR format.

▼ **SNMP V2 Settings**

* Community string:

▼ **SNMP V3 Settings**

*User name:

Authentication protocol: Authentication Password:

Privacy protocol: Privacy Password:

Discover

	Name	IP Address	SNMP Version	Device Details	SNMP Enforcement	Location Group	Default Vlan	
<input type="checkbox"/>	1	<input type="text" value="10.204.88.16"/>	10.204.88.16	V2	Vendor: CISCO Name: Profiler3750 Descr: Cisco IOS Software, C3750 Software (C3750-IPSERV) Location: Bangalore	<input checked="" type="checkbox"/>	initialSetup_snmp	<input type="text" value="123"/>

Add Device

- Discovery of SNMP-enabled devices applies only to L2 and L3 devices which support Bridge MIB configuration.



- Enable the SNMP Enforcement checkbox for using the device for SNMP enforcement and then define the location group and the default VLAN. For Profiler, you must disable SNMP enforcement; the Location Group, Default VLAN fields are not applicable for profiling.

- Admin can modify the added SNMP client to enable the ACL enforcement if required. See

[Adding SNMP Client](#)

Verifying the status of SNMP Devices

You can view the SNMP device status from the SNMP Device page. You can view details such as device name, device location, device description, device contact information, SNMP version, IP Address, model, location group, default VLAN, default ACL, and the current status of the added device.

To view the status of SNMP devices:

1. Select **Endpoint Policy > Network Access > Network Infrastructure Device**.
2. Click **Configuration**.

Network Access > Network Infrastructure Device > Network Infrastructure Device Configuration

Network Infrastructure Device Configuration

RADIUS Dictionary | RADIUS Vendor | Location Group | RADIUS Client | RADIUS Attributes | **Network Infrastructure Device** | SNMP Enforcement Policies

Configuration | Discovery | Templates | ACL

New... Duplicate... Delete... Enable Disable

10 records per page Search:

	Name	Protocol	IP Address	Device Details	Location Group	Default VLAN	Default ACL	Status
<input type="checkbox"/>	1 C2960X uac.local	SNMP-V3	10.254.20.10	Vendor: CISCO Name: C2960X.uac.local Descr: Cisco IOS Software, C2960X Software (C2960X-UNIV... Location: HUBROOM Contact: test	SNMP-LG	60	N.A.	●

Configuring SNMP Enforcement Policy

SNMP Enforcement Policy is used for dynamic VLAN assignment and modification, which is based on role assignment.



You must ensure that the session roaming is enabled on the roles for SNMP enforcement.

To configure an SNMP Enforcement Policy:

1. Select **Endpoint Policy > Network Access > SNMP Enforcement Policies**.
2. Click **New SNMP Policies** to display the New SNMP Policy configuration page.

Network Access > SNMP Enforcement Policies > Full Access Policy

Full Access Policy

▼ SNMP Policy

*Policy Name: Full Access Policy Label to reference this SNMP Policy

Description:

Location Group: SNMP-LG To manage groups, see the [Location Group](#)

*Either VLAN or ACL is mandatory

VLAN: 65

ACL: - Custom - To manage ACLs, see the [ACL](#). If the ACL is directly configured on the switch, select '- Custom -' option.

Custom ACL: Specify the ACL which is directly configured on the switch.

▼ Roles

Policy applies to ALL roles

Policy applies to SELECTED roles

Policy applies to all roles OTHER THAN those selected below

Available roles: Guest, Guest Admin, Guest Sponsor, Guest Wired Restrict, REMEDIATION

Selected roles: ENGG

Add -> Remove

Save Changes

3. On the SNMP policy configuration page:
 - Enter a label for the SNMP enforcement policy.
 - Enter a description for the SNMP policy.
 - For VLAN, specify the VLAN to assign.
 - Choose a location group from the dropdown menu.
 - Under Roles, select Policy Applies to Selected Role; choose a role from the Available Roles and click Add to add it to the Selected Roles list.
4. Click **Save Changes** to save the configuration.

Configuring SNMP Policy Enforcement through Templates using ACL/VLAN

Policy enforcement using ACLs is achieved through both SNMP and SSH. The SNMP traps are received through SNMP and ACL enforcement is done using CLI (SSH).

Template based Policy enforcement using ACL/VLAN as enforcement attribute is achieved through a combination of SNMP and SSH protocols. SNMP protocol is used to receive the traps and ACL/VLAN enforcement is performed using CLI via SSH protocol.

Pre-requisites

- The user must be logged in with highest privilege level for ACL/VLAN enforcement using SSH.
- ACLs should be configured either manually on the Switch or pushed from 182 through ACL creation.
- Default templates are available for Cisco, Juniper and HP. For other Switch models/vendors the admin can create new template. See [Creating Template or using Existing Template](#).
- Enable SNMP diagnostic logging to capture the CLIs sent to the Switch.

Creating Template or using Existing Template

Template is required to specify the CLI format for each vendor. Admin can upload/download the templates which will be in pre-defined format. Using the template, CLIs are formed to enforce the ACL/VLAN on to the interface.

To view and add the templates:

1. Select **Endpoint Policy > Network Access > Network Infrastructure Device > Templates**.



Cisco, Juniper, HP, HP 3com, Dell, Alcatel-Lucent, Arista and Huawei switch templates are available by default.

New Template... Delete... Restore Factory Default...				
10 records per page		Search: <input type="text"/>		
ID	Name	File Name	Vendor	Device Type
1	cisco-switch-i2-enforcer.tpl Template for SNMP policy enforcement with Cisco switches	cisco-switch-i2-enforcer.tpl	Cisco Systems	Switch
2	hp-switch-i2-enforcer.tpl Template for SNMP policy enforcement with HP Procurve switches	hp-switch-i2-enforcer.tpl	HP Procurve	Switch
3	dell-switch-i2-enforcer.tpl Template for SNMP policy enforcement with Dell NXXXX series switches	dell-switch-i2-enforcer.tpl	Dell NXXXX Series	Switch
4	juniper-switch-i2-enforcer.tpl Template for SNMP policy enforcement with Juniper switches	juniper-switch-i2-enforcer.tpl	Juniper Networks	Switch
5	hp-3com-switch-i2-enforcer.tpl Template for SNMP policy enforcement with HP 3Com switches	hp-3com-switch-i2-enforcer.tpl	HP 3Com	Switch
6	arista-switch-i2-enforcer.tpl Template for SNMP policy enforcement with Arista Networks switches	arista-switch-i2-enforcer.tpl	Arista Networks	Switch
7	huawei-switch-i2-enforcer.tpl Template for SNMP policy enforcement with Huawei switches	huawei-switch-i2-enforcer.tpl	Huawei	Switch
8	alcatel-switch-i2-enforcer.tpl Template for SNMP policy enforcement with Alcatel-Lucent switches	alcatel-switch-i2-enforcer.tpl	Alcatel-Lucent	Switch

2. Admin can also choose to create a new template. Click **New Template**.

Network Access > Network Infrastructure Device > Templates > New Template

New Template

* Name: Label to reference this template.

Description:

* Template File: No file chosen Template file

* indicates required field

3. Enter the template name.
4. Enter the description.
5. Click **Browse** and upload the created template file.

6. Click **Save Changes**.

(Optional) Creating an ACL

The Admin can configure ACL in 2 ways:

- Logging into the Switch console and creating the ACLs manually. Ensure that the configured ACL name is same while creating the SNMP client and policy in IPS.
- Creating the ACLs on IPS, which will push the ACLs to the switches belonging to the corresponding Location Group.



Creating an ACL in IPS is not applicable if Enforcement attribute is VLAN.

To create an ACL on IPS:

1. Select **Endpoint Policy > Network Access > ACL**.
2. Click **New ACL**.
3. Enter the Name
4. Enter the ACL number.
5. Set the Location Group.

6. Under ACL Rules:

- Specify the Protocol.
- Enter the Destination IP address
- Enter the Destination Port
- Specify the action as either permit or deny.
- Click **Add**.

Network Access > Network Infrastructure Device > Access Control List (ACL) > 3COM-Default-ACL

3COM-Default-ACL

*Name: Label to reference this ACL.

Number: Applicable only for H3C. Ensure to use the unused ACL number.

Description:

*Location Group: To manage groups, see the [Location Group](#)

▼ ACL Rules

<input type="checkbox"/>	Protocol	Destination IP / Network	Destination Port	Action	
<input type="checkbox"/>	<input type="text" value="ip"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="permit"/>	<input type="button" value="Add"/>
<input type="checkbox"/>	ip	10.20.100.10		permit	
<input type="checkbox"/>	ip	0.0.0.0/0		deny	

7. Click **Save Changes**.

- Admin can login to the Switch and verify if the ACL is properly configured. ACL name is prefixed with IPS- to distinguish between the ACLs created manually and the one's pushed from IPS.

- ACL name modification is not allowed.

- When deleting an ACL from IPS ensure that it is not applied on any interface or port.



Otherwise, deletion of ACL will not succeed on the Switch.

- ACL configured from IPS should not be modified manually.

- ACL number has to be chosen based on the *Switch configuration guide*. This is required only for the Switches, which create ACLs using ACL number as the key. Ensure that the configured ACL number is not used on the Switch. Currently, ACL number is mandatory only for HP-3com (H3C) switches.

- Alcatel-Lucent Switch (Omni-Switch) doesn't support ACL configuration on the interface. Hence, ACL enforcement is not supported for Alcatel-Lucent Switch (Omni-Switch).

Adding SNMP Client

To add a client using ACL enforcement:

1. Select **Endpoint Policy > Network Access > Network Infrastructure Device**.
2. Click **New**.
3. Enter the name of the client that will be added in the IPS.
4. Enter the description.
5. Enter the IP address of the client.
6. Under Enforcement, select **ACL Enforcement**.



ACL enforcement is supported for all Switches supporting SSH.

7. Select the Location Group.
8. Select default ACL from the drop down.



Select the Custom option and enter the ACL name if the ACL is configured manually on the Switch.

9. Select the template corresponding to the selected vendor.
10. Under SSH settings:
 - Specify the Authentication Method.
 - Enter the user name, password and port number if authentication method is Password OR
 - Enter the user name, key and pass-phrase if the authentication method is Public Key.
11. Under SNMP settings, specify the SNMP version.
12. Specify the Read username, Read Security Level, Auth Protocol, and Auth Password.
13. Click **Save Changes**.

Network Access > Network Infrastructure Device > New Network Infrastructure Device

New Network Infrastructure Device

*Name: Label to reference this Device.

Description:

*IP Address: IP Address of this Device.

*Vendor: Device Vendor.

Enforcement

ACL and/or VLAN will be used as an enforcement attribute to provision the policy for the endpoint. VLAN Enforcement is supported only for HP and Cisco.
Enforcement is supported only for Wired Switches.

ACL Enforcement VLAN Enforcement

*Location Group: Only groups which are associated with a MAC Address realm appear here. To manage groups, see the [Location Group](#)

*Default ACL: To set restricted ACL on the interface when no user is connected or no ROLE assigned to the user. To manage ACLs, see the [ACL](#). If the ACL is directly configured on the switch, select "- Custom -" option.

*Custom ACL: Specify the ACL which is directly configured on the switch.

*Template: Template used for SSH enforcement

SSH Settings

Authentication Method: *Use Public key authentication to maximize security

*User:

*Password:

Port Number: SSH port number

SNMP Settings

*SNMP Version: v1N2c v3

Same credentials for Trap user

*Read Username:

*Read Security Level:


*Auth Protocol:

*Auth Password: Minimum 8 characters.



Admin can select both VLAN and ACL enforcement for an SNMP client.

To add a client using VLAN enforcement:

1. Select **Endpoint Policy > Network Access > Network Infrastructure Device**.
 2. Click **New**.
 3. Enter the name of the client that will be added in the IPS.
 4. Enter the description.
 5. Enter the IP address of the client.
 6. Under Enforcement, select **VLAN Enforcement**.
-
-  VLAN enforcement using SSH is supported on all Switches except HP and Cisco.
-
7. Select the Location Group.
 8. Enter the default VLAN number.
 9. Select the template corresponding to the selected vendor.
 10. Under SSH settings:
 - Specify the Authentication Method.
 - Enter the user name, password and port number if authentication method is Password OR
 - Enter the user name, key and pass-phrase if the authentication method is Public Key.
 11. Under SNMP settings, specify the SNMP version.
 12. Specify the Read username, Read Security Level, Auth Protocol, and Auth Password.

13. Click **Save Changes**.

Network Access > Network Infrastructure Device > Dell-switch-N3024

Dell-switch-N3024

*Name: Label to reference this Device.

Description:

*IP Address: IP Address of this Device.

*Vendor: Device Vendor.

Enforcement

ACL and/or VLAN will be used as an enforcement attribute to provision the policy for the endpoint.
Enforcement is supported only for Wired Switches.

ACL Enforcement VLAN Enforcement

*Location Group: Only groups which are associated with a MAC Address realm appear here. To manage groups, see the [Location Group](#)

*Default VLAN: To set the device interface to default VLAN specified value when there is no ROLE assigned. This is mainly used when a SNMP session is deleted

*Template: Template used for SSH enforcement

SSH Settings

Authentication Method:

*Use Public key authentication to maximize security

*User:

*Password:

Port Number: SSH port number

SNMP Settings

*SNMP Version: v1/v2c v3

Same credentials for Trap user

*Read Username:

*Read Security Level:

*Auth Protocol:

*Auth Password: Minimum 8 characters.

*Priv Protocol:

*Priv Password: Minimum 8 characters.

SNMP Enforcement Policies

To create SNMP Enforcement policies:

1. Select **Endpoint Policy > Network Access > SNMP Enforcement Policies**
2. Click **New Policy**.
3. Enter the policy name.
4. Enter the Description.
5. Select the Location Group.

6. Select the ACL from the drop down.



Select the Custom option and enter the ACL name if the ACL is configured directly on the Switch.

7. Under Roles, specify:

- Policy applies to ALL roles-To apply the policy to all users.
- Policy applies to SELECTED roles-To apply this policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
- Policy applies to all roles OTHER THAN those selected below-To apply this policy to all users except for those who map to the roles in the Selected roles list. You must add roles to this list from the Available roles list.

8. Click **Save changes**.

Network Access > SNMP Enforcement Policies > New SNMP Enforcement Policy

New SNMP Enforcement Policy

▼ **SNMP Policy**

*Policy Name: Label to reference this SNMP Policy.

Description:

Location Group: To manage groups, see the [Location Group](#)

*Either VLAN or ACL is mandatory

VLAN:

ACL: To manage ACLs, see the [ACL](#). If the ACL is directly configured on the switch, select '- Custom -' option.

▼ **Roles**

Policy applies to ALL roles

Policy applies to SELECTED roles

Policy applies to all roles OTHER THAN those selected below

Available roles:
Guest Admin
Guest Sponsor
Guest Wired Restrict
Users

Selected roles:



Either VLAN and/or ACL must be configured in the SNMP policy.

Appendix

Configuration Commands for Cisco

The following is a sample configuration for linkup/linkdown/MAC notification traps for SNMP v2c. In the below configuration snmp server is configured as IPS, which is receiving SNMP traps.

You must execute the following commands in configuration mode.

```
Execute the following command to globally enable linkup and linkdown traps.
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification
Execute the following command to configure IPS as an snmp-server host, which receives
SNMP notifications.
snmp-server host <IPS IP Address> trap version 2c public snmp mac-notification
mac-address-table notification interval 0
mac-address-table notification
mac-address-table aging-time 3600
snmp-server community string ro
snmp-server community string rw
```

Cisco SNMP v3 configuration

The following commands show a sample configuration for configuring SNMP v3 on Cisco switch. In the below configuration snmp server is configured as IPS, which is receiving SNMP traps.

You must execute the following commands in configuration mode.

```
snmp-server view <Read-View Name> iso included
snmp-server view <Write-View Name> iso included
The below configuration applies when the SNMP v3 settings for Security Level is "Auth,
Prev" on IPS.
snmp-server group <snmpv3 group name> v3 priv context vlan- match
snmp-server group <snmpv3 group name> v3 priv read <Read-View Name> write <Write-View
Name>
snmp-server user <snmpv3 username> <snmpv3 group name> v3 auth sha/md5 <auth password>
priv aes/des <128> <password>
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server host <IPS IP Address> version 3 auth/priv <snmpv3 username> snmp
```

The below configuration applies when the SNMP v3 settings for Security Level is "Auth, NoPrev" on IPS.

```
snmp-server group <snmpv3 group name> v3 auth read <Read-View Name> write <Write-View Name>
snmp-server group <snmpv3 group name> v3 auth context vlan- match prefix
snmp-server user <snmpv3 username> <snmpv3 group name> v3 auth sha/md5 <auth password>
snmp-server host <IPS IP Address> version 3 auth <snmpv3 username>
```

The following sample shows the command, which are executed at interface level.

```
switchport mode access
switchport access vlan 4
snmp trap mac-notification added
```

Configuring Port Security Traps

The following sample shows the commands that is executed at global set up level for configuring port security traps.

```
snmp-server enable traps port-security
snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.1.5 version 2c public port-security
The following sample shows the commands, which are executed at interface level.
switchport access vlan <default vlan>
switchport port-security
switchport port-security maximum 2
switchport port-security maximum 1 vlan access
switchport port-security violation restrict
switchport port-security mac-address <dummy mac address>
```

Configuring Cisco ACL

The following sample shows the command for default ACL.

```
#show ip access-lists snmp-default-acl
Extended IP access list snmp-default-acl
  10 deny ip any any
#show run int gi 1/0/7
interface GigabitEthernet1/0/7
The default ACL is pushed from IPS
  ip access-group <Default-ACL>
end
The following sample shows the command for Restrict ACL.
```



```
#show ip access-lists snmp-restrict-acl
Extended IP access list snmp-restrict-acl
  10 permit tcp any host <IPS-IP Address>
  20 permit tcp any host <IPS-IP Address> eq 443
  30 permit tcp any host <IPS-IP Address> eq www
  100 deny ip any any
#show run int gi 1/0/7
interface GigabitEthernet1/0/7
The Restrict ACL name is pushed from IPS.
  ip access-group <restrict-ACL name>
end
```

The following sample shows the command for Full Access ACL.

```
#show ip access-lists snmp-full-access-acl
Extended IP access list snmp-full-access-acl
  10 permit ip any any
#do sh run int gi 1/0/7
interface GigabitEthernet1/0/7
The Full access ACL is pushed from IPS
ip access-group <Full-Access-ACL name>
end
```

Configuration Commands for Juniper

Juniper SNMP v2 Configuration

```
set snmp client-list listnew <IPS-IP>
set snmp community public authorization read-write
set snmp community public client-list-name listnew
set snmp trap-group global
set groups global snmp trap-group managers version v2
set groups global snmp trap-group managers targets <IPS-IP>
```

Juniper SNMP v3 Configuration

```
set snmp v3 usm local-engine user <user-name> authentication-sha authentication-key
<key>
set snmp v3 usm local-engine user <user-name> privacy-aes128 privacy-key <key>
set snmp v3 vacm security-to-group security-model usm security-name <user-name> group
<group name>
```

```
set snmp v3 vacm access group <group name> default-context-prefix security-model any
security-level privacy read-view view-all
set snmp v3 target-address tarallow address <IPS-IP>
set snmp v3 target-address tarallow tag-list MYTAG
set snmp v3 target-address tarallow address-mask 255.255.255.255
set snmp v3 target-address tarallow target-parameters <target parameter name>
set snmp v3 target-parameters tp1 parameters message-processing-model v3
set snmp v3 target-parameters tp1 parameters security-model usm
set snmp v3 target-parameters tp1 parameters security-level privacy
set snmp v3 target-parameters tp1 parameters security-name <user-name>
set snmp v3 target-parameters tp1 notify-filter NF1
set snmp v3 notify N1 type trap
set snmp v3 notify N1 tag MYTAG
set snmp v3 notify-filter NF1 oid 1.3.6.1.6.3.1.1.5.3 include
set snmp v3 notify-filter NF1 oid 1.3.6.1.6.3.1.1.5.4 include
```

Configuration Commands for Dell

SNMP v2 Configuration

```
snmp-server view <SNMP label> iso included
snmp-server community "public" rw
snmp-server host <IPS-IP> traps version 2 "public"
```

SNMP V3 Configuration

```
snmp-server view "profiler" iso included
snmp-server filter "profiler" iso included
snmp-server group <group name> v3 auth read "profiler" write "profiler"
snmp-server group <group name> v3 priv notify "profiler" read "profiler" write
"profiler"
snmp-server user <user-name> <group name> auth-md5-key <key> priv-des-key <key>
snmp-server v3-host <IPS-IP> <user name> traps priv
```

Configuration Commands for HP 3Com

HP 3Com SNMP v2 Configuration

```
snmp-agent community read public
snmp-agent sys-info version v2c
```

```
snmp-agent target-host trap address udp-domain <IPS-IP> params securityname public v2c
```

HP 3Com SNMP v3 Configuration

```
snmp-agent community read public
snmp-agent sys-info version all
snmp-agent group v3 <Group name>
snmp-agent target-host trap address udp-domain <IPS-IP> params securityname public v3
privacy
snmp-agent usm-user v3 <user name> <Group name> cipher authentication-mode md5 <key>
privacy-mode des56 <key>
snmp-agent trap enable default-route
```

Configuration Commands for HP

HP SNMPv2 Commands

The following is a sample configuration for MAC notification traps for SNMP v2c. In the below configuration snmp server is configured as IPS, which is receiving SNMP traps. Execute the following commands.

```
snmp-server community "public"
snmp-server community "private" unrestricted
snmp-server host 10.204.89.131 community "public" trap-level all
```

The following command shows an example for configuring linkup, linkdown, and MAC notification traps.

```
--Execute the following commands for enabling linkup and linkdown traps.
snmp-server enable traps link-change 5
--Execute the following command for enabling mac notification.
snmp-server enable traps mac-notify
```

HP SNMPv3 Commands

The following commands show a sample configuration for configuring SNMP v3 on switch. In the below configuration snmp server is configured as IPS, which is receiving SNMP traps.

Execute the following commands in configuration mode.

```
snmpv3 enable
snmpv3 only
snmpv3 restricted-access
```

```
snmpv3 group managerpriv user sec-model ver3
snmpv3 notify "procurve" tagvalue "procurve"
snmpv3 targetaddress "procurve" params "procurve" 10.204.xx.xxx filter all taglist
"procurve"
snmpv3 params "procurve" user sec-model ver3 message-processing ver3 priv
snmpv3 community index "20" name "public" sec-name tag "procurve"
snmpv3 user
no snmpv3 user initial
```

The following command shows an example configuration for configuring port security trap.

```
snmp-server enable traps port-security
```

ACL Configuration for Default, Restricted, and Full Access Role

Restricted ACL, give access to DHCP server and IPS

```
ip access-list extended <"Remediation-ACL">
10 permit udp <Source-Address><wildcard/mask> eq <port number> <Destination-Address>
<wildcard/mask> eq <port number>
20 permit tcp 0.0.0.0 255.255.255.255 10.204.xx.x 0.0.0.0 eq 443
30 permit tcp 0.0.0.0 255.255.255.255 10.204.xx.x 0.0.0.0 eq 80
exit
ip access-list extended <"Default-ACL-Name">
10 deny 0.0.0.0 255.255.255.255
exit
ip access-list extended <"Full-Access-ACL">
10 permit 0.0.0.0 255.255.255.255
exit
```

Configuration Commands for Alcatel-Lucent

Alcatel-Lucent SNMP V2 Configuration

The following is a sample configuration for MAC notification traps for SNMP v2c. In the below configuration snmp server is configured as IPS, which is receiving SNMP traps.

```
snmp-user pulse password juniper123 read-only all no auth
snmp community map public user pulse
user secure password juniper123 read-write all no auth
snmp community map private user secure
snmp security no security
snmp station 10.96.xx.x secure v2 enable
```

Alcatel-Lucent SNMP V3 Configuration

```
aaa authentication snmp local
user snmpv3user password juniper123 md5+des read-write all
user snmpv3user password juniper123 md5+des read-write all priv-password fjf
snmp community map "public" user "snmpv2user" on
snmp security authentication set
snmp station 10.10.10.10 162 "snmpv3user" v3 enable
```

Configuration Commands for Arista

Arista SNMP V2 Configuration

```
snmp-server community public rw
snmp-server host 10.96.xx.xx version 2c public
snmp-server enable traps snmp authentication
snmp-server enable traps snmp link-down
snmp-server enable traps snmp link-up
```

Arista SNMP V3 Configuration

SNMP V3: AuthNoPriv: Arista

```
Command for configuring the Switch: tacacs-switch(config)#snmp-server user
authnoprivsha TEST_GROUP v3 auth sha Psec
tacacs-switch(config)#show running-config | include snmp
snmp-server engineID local xxxxxx
snmp-server local-interface Management1
snmp-server view all-items iso included
snmp-server group TEST_GROUP v3 auth write all-items
snmp-server user <user-name>authnoprivsha TEST_GROUP v3 localized xxxx auth sha 6dasda
snmp-server host 10.96.xx.xx version 3 auth <user-name>authnoprivsha
snmp-server enable traps snmp authentication
snmp-server enable traps snmp link-down
snmp-server enable traps snmp link-up
```

SNMP V3: AuthPriv: Arista

```
tacacs-switch#sho running-config | include snmp
snmp-server engineID local xxxxxx
snmp-server local-interface Management1
snmp-server view all-items iso included
```

```
snmp-server group TEST_GROUP v3 priv write all-items
snmp-server user <user-name>md5 TEST_GROUP v3 localized xxxxx auth md5 cxc priv des
3adada
snmp-server user <user-name>md5aes TEST_GROUP v3 localized xxxxx auth md5 7dada priv
aes c4dsdf
snmp-server user <user-name>shaaes TEST_GROUP v3 localized xxxxx auth sha 49da priv
aes 3dasd
snmp-server user <user-name>shades TEST_GROUP v3 localized xxxx auth sha 6das priv des
af95
snmp-server host 10.96.xx.xx version 3 priv md5
snmp-server enable traps snmp authentication
snmp-server enable traps snmp link-down
snmp-server enable traps snmp link-up
```

Configuring ACL

ACL Configuration for Default, Restricted, and Full Access Role

```
#show running-config
ip access-list <FullAccess_ACL>
  1 permit ip any host 10.x.x.x
  3 permit icmp any host 10.100.x.x
  4 deny ip any host 0.0.0.0
!
ip access-list <RestrictedAccess_ACL>
  1 permit ip any host 10.200.200.200
  2 permit ip any host 10.100.100.100
  3 permit icmp deny host x.x.x.x
  4 deny ip any host 0.0.0.0
!
ip access-list <BlockAllTraffic_ACL>
  1 deny ip any host 0.0.0.0
```

Configuration Commands for Huawei

Huawei SNMP V2 Configuration

```
snmp-agent
snmp-agent local-engineid casdasd
snmp-agent community read cipher xxxx
snmp-agent community write cipher xxxx
```

```
snmp-agent community complexity-check disable
snmp-agent sys-info version all
snmp-agent target-host trap address udp-domain 192.168.xx.xx params securityname
cipher xxx
snmp-agent mib-view included allextgmp iso
snmp-agent mib-view excluded allextmon rmon
snmp-agent notification-log enable
snmp-agent notification-log global-ageout 12
snmp-agent trap enable
```

Huawei SNMP V3

```
[Huawei]display current-configuration | include snmp
snmp-agent
snmp-agent local-engineid xxxx
snmp-agent sys-info version v3
snmp-agent group v3 snmpv3group authentication
snmp-agent group v3 snmpv3group privacy read-view isoview write-view isoview notify-
view isoview
snmp-agent target-host trap address udp-domain 192.168.xx.xx params securityname
snmpv3user v3 privacy
snmp-agent mib-view included isoview iso
snmp-agent mib-view excluded allextmon rmon
snmp-agent usm-user v3 snmpv3user
snmp-agent usm-user v3 snmpv3user group snmpv3group
snmp-agent usm-user v3 snmpv3user authentication-mode md5 cipher xxx
snmp-agent usm-user v3 snmpv3user privacy-mode aes128 cipher xxx
snmp-agent notification-log enable
snmp-agent notification-log global-ageout 12
snmp-agent trap enable
```

Configuring ACL

ACL Configuration for Default, Restricted, and Full Access Role

```
-----
display acl all
(In Restricted ACL, give access to DHCP server and IPS)
Advanced ACL restrictedAccess 3997, 3 rules
rule 1 permit tcp destination <IPS_IP> <wildcard> destination-port eq 443
rule 2 permit udp destination-port eq bootpc
```

```
rule 3 permit udp destination-port eq 80
```

```
Advanced ACL fullAccess 3998, 1 rule
```

```
rule 1 permit ip destination 0.0.0.0 <wildcard>
```

```
Advanced ACL defaultAccess 3996, 1 rule
```

```
rule 1 deny ip destination 0.0.0.0 <wildcard>
```


Policy Enforcement using 802.1X Native Supplicant

Overview

IPS supports 801.X authentication using native supplicants. The Native supplicant is the default Operating System (OS) agent, which runs on the client machine. The mobile platforms and laptops have native supplicant support.



The secondary authentication is not supported with 802.1x Native supplicant.

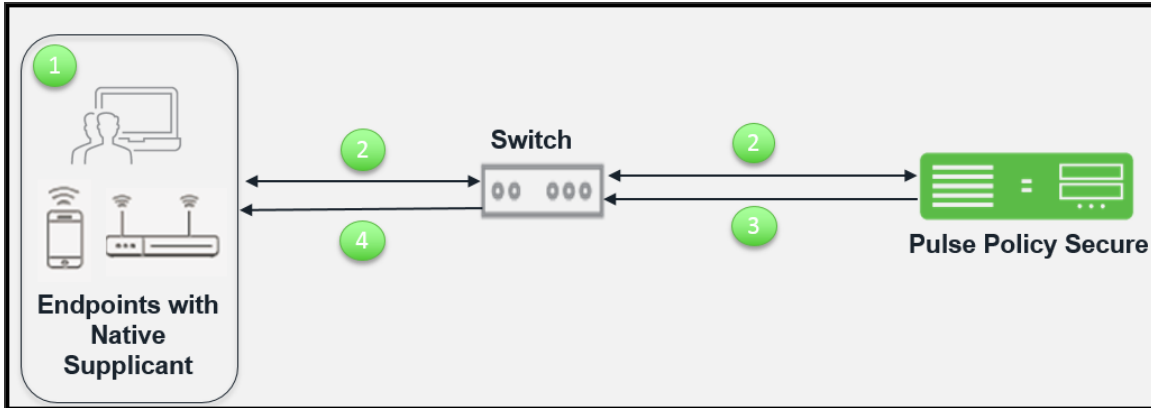
Benefits

- Supports simplified access to applications from personally owned devices, addressing the Bring Your Own Device (BYOD) users.
- Devices that do not have Pulse Client can authenticate with IPS and get the realm and roles applied.

Deployments using 802.1X Authentication with Native Supplicant

802.1X Authentication with Native Supplicant

Using IPS, you can provision 802.1X authentication for endpoints using native supplicant. The Layer 2 authentication and enforcement is used to control network access policies at the edge of the network using an 802.1X enabled switch or access point.



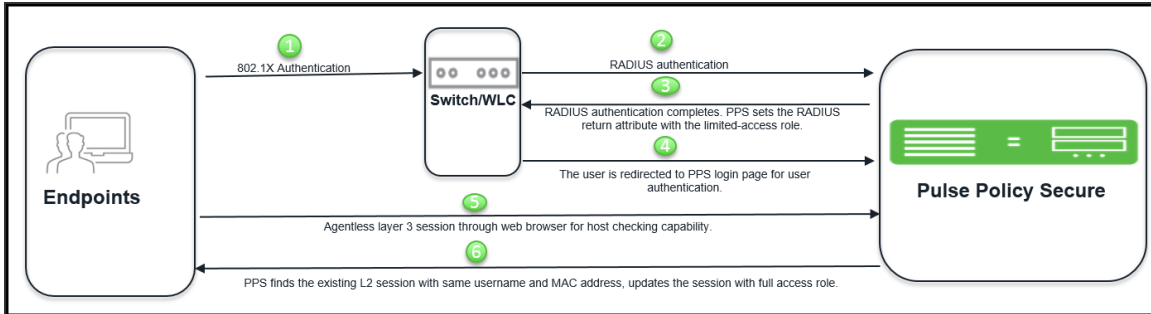
The workflow for 802.1X authentication with native supplicant is described below:

1. Configure the endpoints protocols from the Adapter settings as per the IPS configured protocols. Once the client adapter is online the authentication starts automatically.
2. Switch receives the request and starts RADIUS authentication with IPS. The user is prompted for user credentials.
3. IPS assigns the roles based on the credentials provided by the user. IPS communicates the enforcement rules to switch in form of RADIUS return attributes (For example, Change of VLAN) for the authenticated user.
4. Switch provides access and IP address to the endpoints based on the RADIUS return attributes.

Agentless Host Checking with Native Supplicant

As many users bring their own devices, additional intelligence must be applied to eliminate intrusions and protect sensitive information. The IT administrators need the ability to control where devices are allowed on the network, based on the device type, operating system, owner of the device and user log in credentials of the device. The network resource request must be handled appropriately and appropriate action must be taken for any violation, which includes limiting access to internet only.

The IPS solution provides endpoint compliance for BYOD devices for providing seamless access to protected resources with native supplicant. For example, enterprise users need to provide onsite access to employees and contractors. To provide network access, the BYOD devices from contractor must be compliant to host checker security policies. For such users, you can use 802.1X authentication using native supplicant and then endpoint compliance check is achieved using a web browser. A single session is created for both the connections and a single license is consumed.



The workflow is described below:

1. The contractor user connects to network, performs layer 2 authentication using AD credentials. For 802.1X, AD username and password is used for authentication. For MAC authentication, endpoints MAC address or device attributes for profiler is used for authentication.
2. The endpoint host check is not performed and hence the user gets limited connectivity. The user must be compliant to host check security policy for full access.
3. IPS sets the RADIUS return attribute with limited access role. Limited access role is applied on the endpoint.
4. The user is redirected to a IPS log in page for user authentication.
5. The user opens the web browser and enters the AD username and password. The agentless Host Checker provides the compliance details to IPS.
6. IPS finds the existing session with the same username and MAC address and then updates the session with full access role.

The user gets the required full access to protected resources if the system is compliant to HC security policies.



- The user can choose to remember the username and password to avoid entering it multiple times for layer 2 and layer 3 connections.
- This feature is supported for Windows and MAC OSX.
- For configuration, see [Configuring Agentless Host Checking with Native Supplicant](#) .

Host Checking with Native Supplicant

On Mac OSX, Windows, and Linux endpoint using native supplicant, IPS Host checking can be enforced only for Layer 3 connection. Once the endpoint gets authenticated using native supplicant and gains network access, you can launch and install Pulse Client using web browser deployment or SCCM advertisement to establish a Layer 3 session. This evaluates the health status of the endpoints and thereby ensuring legitimate resource access behind IPS Enforcer.

There will be only one session for Layer 2 and Layer 3 connections on IPS which will consume single license.

For agentless host checking, native supplicant is used to perform 802.1x authentication. The compliance check is performed using browser based agentless L3 session. The L2 and agentless L3 session are bridged on IPS to provide compliance based layer 2 access control. For access control, RADIUS return attribute Filter-ID with Radius COA is used.

The Host Checker functionality is not supported on the native Mozilla browser on MAC OSX. As a workaround disable the Captive Network Assistant feature, which is enabled by default or open the Pulse Client using a different web browser.



Using Native Supplicant the Host Checker functionality is not supported. This is possible through [Configuring Agentless Host Checking with Native Supplicant](#) .

Agentless Session Bridging requires Host Checker functionality to be executed on Linux via JAVA NPAPI plugin, which is only supported on Firefox ESR browser with v52.0 and lower.

Configuring Agentless Host Checking with Native Supplicant

The access control for this use case can be achieved through RADIUS CoA and a sample workflow is described below:

1. The native supplicant performs 802.1X authentication and IPS creates a session. The IPS assigns a limited access role since the host check is not performed.

- The user configures the RADIUS URL-redirection attributes on the Cisco Switch. Using RADIUS URL-Redirection return attributes the Cisco switch redirects any initial HTTP/s traffic to IPS so that Layer 3 authentication is performed along with compliance check. Upon successful Host Check, a different set of radius attributes is pushed using Radius CoA to seamlessly access any resource.

You must configure the following return attributes (supported only on Cisco switches):

```
Cisco-AVPAIR=url-redirect-acl=REDIRECT_To_IPS
```

```
Cisco-AVPAIR=url-redirect=https://<IPS-SIGN-IN-URL>/
```

The following figure shows a sample IPS configuration for URL-redirection on Cisco switch.

RADIUS Attributes

Open port

VLAN: (1 - 4094)

Return Attribute: Delete ↑ ↓

Return Attribute	Radius Auth Server Attribute Value	Auth Server Catalog Attribute Value	Value	
Filter-Id	-none-	-none-	<input type="text"/>	Add
Filter-Id	-none-	-none-	<input type="text"/>	✓ ✕
Cisco-AVPAIR	-none-	-none-	url-redirect=https://10.204.8...	✓ ✕

Add Session-Timeout attribute with value equal to the session lifetime

Add Termination-Action attribute with value equal 1

Interface

Roles

Policy applies to ALL roles

Policy applies to SELECTED roles

Policy applies to all roles OTHER THAN those selected below

Available roles:

Selected roles:

Add -> Remove

NOTE: changes to this page will cause all L2 clients to drop their connections and reconnect.

Save Changes Save as Copy

- The user configures the RADIUS CoA attributes. The recommended radius return attribute to perform access control using RADIUS CoA is Filter-ID for wired devices and ACL-name for WLC.

You must configure the following return attributes on IPS:

```
Filter-Id=PERMIT-ALL.in
CiscoAVPAIR=subscriber:command=reauthenticate
Cisco-AVPAIR=subscriber:reauthenticate-type=last
```

The following figure shows a sample IPS configuration for RADIUS CoA.

ID	Name	Attributes	Location Group	Interface	Applies to role
1.	contractor-policy-wireless	ACL-Name=PERMIT-ALL Cisco-AVPAIR=subscriber:command=reauthenticate Cisco-AVPAIR=subscriber:reauthenticate-type=last	WIRELESS-LG	N/A	contractor
2.	contractor-policy-wired	Filter-Id=PERMIT-ALL.in Cisco-AVPAIR=subscriber:command=reauthenticate Cisco-AVPAIR=subscriber:reauthenticate-type=last	WIRED_LG	N/A	contractor
3.	remediation-policy	Cisco-AVPAIR=url-redirect-acl=REDIRECT-IQ Cisco-AVPAIR=url-redirect=https://10.204.89.171/test Session-Timeout=43400 Termination-Action=1	WIRED_LG WIRELESS-LG	N/A	remediation

- The agentless L3 authentication is done through web browser and host check is performed. If host check passes the user receives new role (for example, full-access), which provides full access to authorized resources.

- The L2 and L3 connections are merged and the merged session receives full-access role.
- The change of role triggers new RADIUS return attribute policy. The new policy triggers RADIUS CoA and applies new radius attribute, which provides full access to authorized resources.
- VLAN change using CoA is not supported with Cisco Switches. It is recommended to use RADIUS disconnect for VLAN change.
- The RADIUS CoA configuration for various Cisco switch platforms is described below.



Cisco Platform	IOS Version	RADIUS CoA Configuration
3850	16.3	Filter-Id=PERMIT-ALL.in
2960X	15.2	Filter-Id=PERMIT-ALL.in
2960	12.2	Filter-Id=PERMIT-ALL.in Cisco-AVPAIR=subscriber:command=reauthenticate Cisco-AVPAIR=subscriber:reauthenticate-type=last

Configuring 802.1X for Native Supplicant on IPS

This section covers the procedure for configuring 802.1X authentication on IPS.



- Authentication Protocol Set configuration varies among different platforms. For example, MAC OSX supports EAP-TTLS/PAP, EAP-TTLS/MS-CHAP-V2 and PEAP/EAP-MS-CHAP-V2 authentication protocol set when IPS is configured with AD server for user authentication.
- EAP-TTLS/CHAP are supported with local authentication server and not supported on Active Directory.

Configuring Native Supplicant for 802.1X Authentication

Example: Configuring Windows 7 Native Supplicant for IPS 802.1X Authentication

The 802.1X wired LAN Authentication gives you the possibility to connect your device using the cable network (wired). You can use the windows native supplicant for 802.1X authentication.

Requirements

- Your device must be equipped with a LAN interface and meet the standards for connecting to enterprise networks requiring 802.1X authentication.
- Local admin privileges are required on the endpoint.
- The OS security updates are installed and an Antivirus Software is present and up-to-date.
- It is recommended to disable all third-party connection management tools so that the native Windows tool is used.

Configuring the Windows Native Supplicant

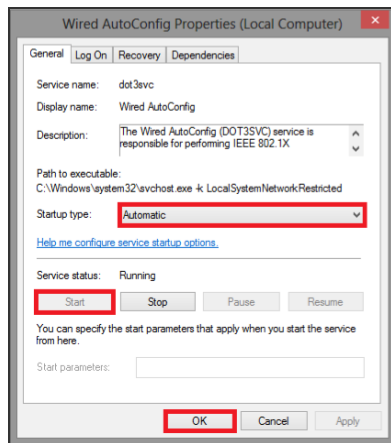
To configure the native supplicant:

1. Select **Control Panel > System and Security > Administrative Tools** and access the Services tool.

In the services window locate the service named **Wired Autoconfig** and double click the service.

WinHTTP Web Proxy Auto-...	WinHTTP i...	Running	Manual	Local Service
Wired AutoConfig	The Wired ...	Running	Automatic	Local Syste...
WLAN AutoConfig	The WLANS...	Running	Automatic	Local Syste...

2. Select the Startup type **Automatic** and click **Start**.

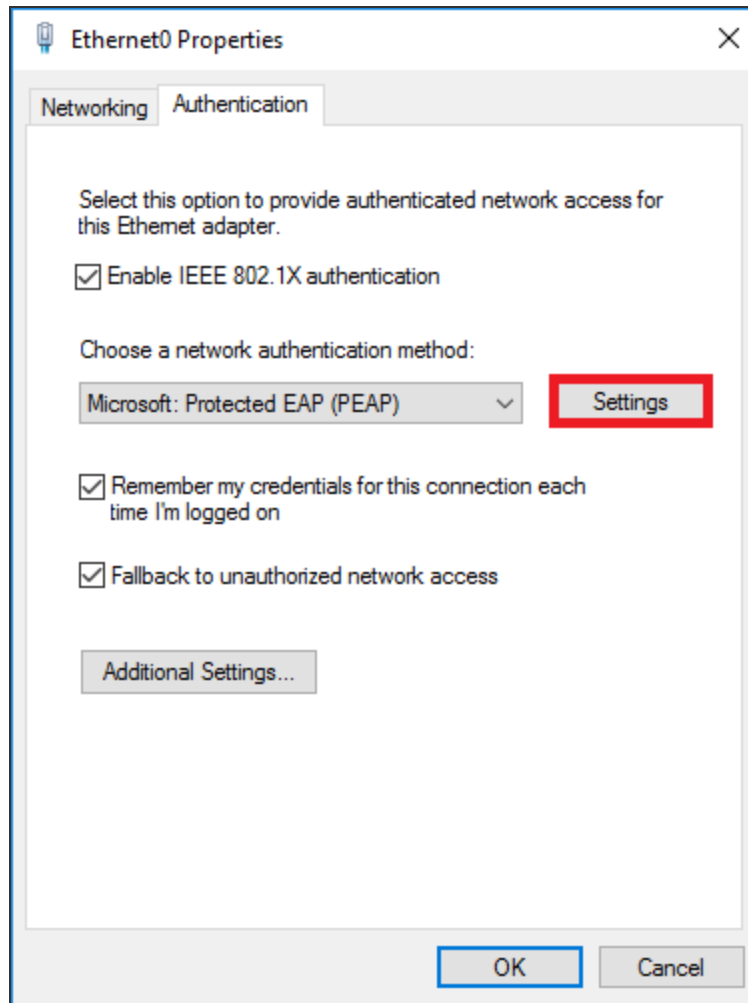


3. Click **Start > Control Panel > Network and Internet > Network and Sharing Center**.
4. Select **Change adapter settings** and then right click on the LAN adapter, Ethernet or Local Area Connection and select Properties.
5. Click the **Authentication** tab at the top of the window. Select **Enable IEEE 802.1X authentication and fallback to unauthorized network access**. From the dropdown list about the network authentication, choose Microsoft: Protected EAP (PEAP).

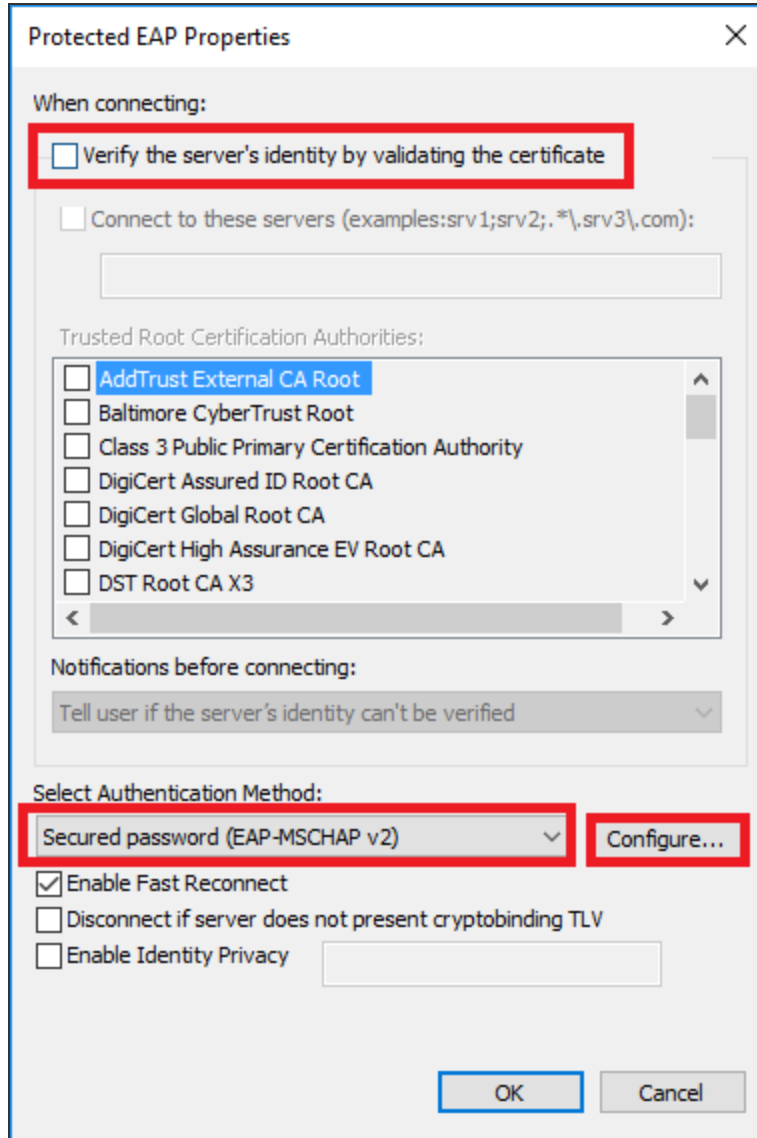
- Click **Settings** to choose the authentication method and then click OK to proceed.



If you choose **Remember my credentials for this connection each time I'm logged on the user credentials** are not prompted for every log in. Don't use this option if multiple people are using the device.



7. Uncheck **Verify the server's identity by validating the certificate** and select the **Enable Fast Reconnect** option. Click **Configure** to continue.



The screenshot shows the "Protected EAP Properties" dialog box. The "When connecting:" section has the checkbox "Verify the server's identity by validating the certificate" unselected. The "Trusted Root Certification Authorities:" list includes "AddTrust External CA Root" (selected), "Baltimore CyberTrust Root", "Class 3 Public Primary Certification Authority", "DigiCert Assured ID Root CA", "DigiCert Global Root CA", "DigiCert High Assurance EV Root CA", and "DST Root CA X3". The "Notifications before connecting:" dropdown is set to "Tell user if the server's identity can't be verified". The "Select Authentication Method:" dropdown is set to "Secured password (EAP-MSCHAP v2)", and the "Configure..." button is visible. The "Enable Fast Reconnect" checkbox is checked, while "Disconnect if server does not present cryptobinding TLV" and "Enable Identity Privacy" are unchecked. The "OK" and "Cancel" buttons are at the bottom.

Protected EAP Properties

When connecting:

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1;srv2;.*\,srv3\,com):

Trusted Root Certification Authorities:

- AddTrust External CA Root
- Baltimore CyberTrust Root
- Class 3 Public Primary Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert High Assurance EV Root CA
- DST Root CA X3

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

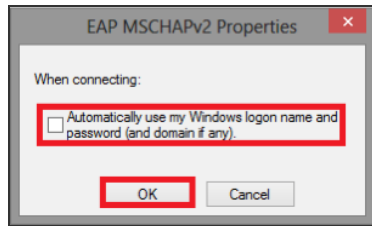
Enable Fast Reconnect

Disconnect if server does not present cryptobinding TLV

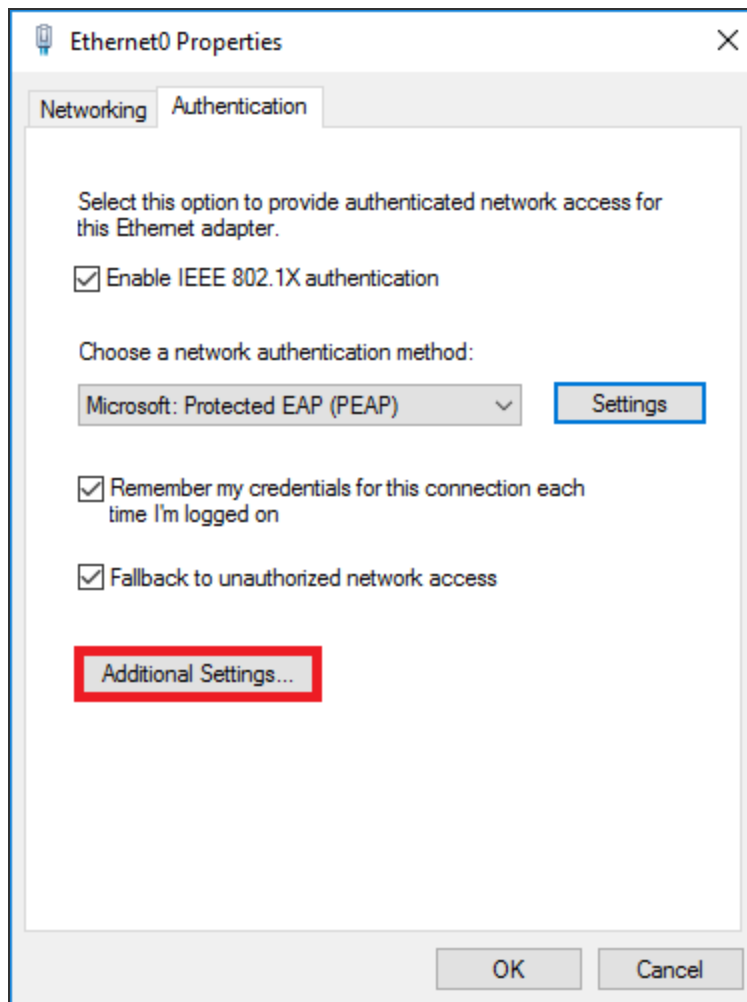
Enable Identity Privacy

OK Cancel

- Uncheck **Automatically use my Windows logon name and password** and click **OK** to confirm.

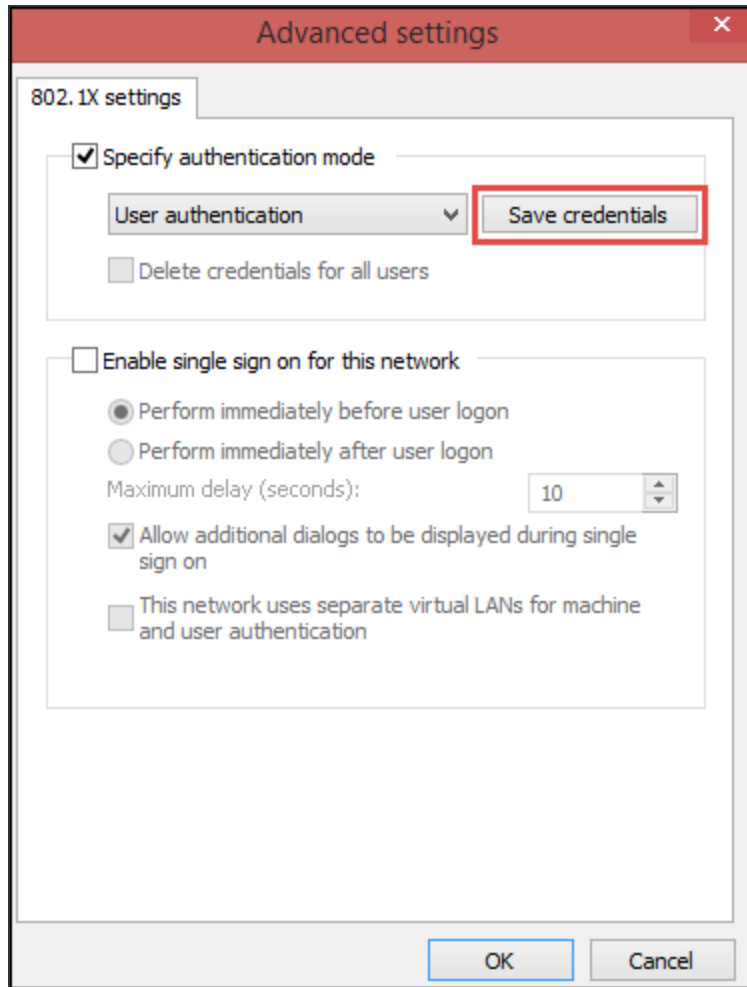


- Click **Additional Settings**.

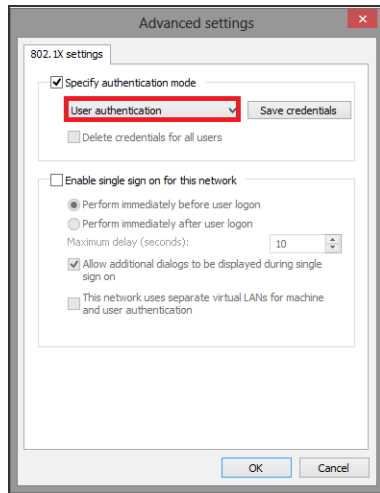


- Select **Specify authentication mode** and choose **User authentication** from the list.

11. If you are using Cisco switch/WLC then you can use Save credentials to save the user credentials.



- Click **Additional Settings** and choose **User authentication** and then Click **OK**.



- Plug the network cable and If already inserted, unplug it and attach it again.
- A log in window pops to enter **Username** and **Password**.

Example: Configuring Mac OSX Native Supplicant for IPS 802.1X Authentication

This section details the procedure for configuring native Mac OSX supplicant for IPS 802.1X authentication.

Requirements:

- Apple Mac OSX endpoint
- iPhone Configuration utility

Configuring MAC OSX Native Supplicant

Authentication to a IPS 802.1X server in MAC OSX endpoints is achieved using Apple Configurator. This tool allows you to easily create, maintain, and install configuration profiles, track and install provisioning profiles, and capture device information including console logs.



The latest MAC OSX endpoints can be configured using Apple Configurator 2 tool.

Configuring 802.1x profile

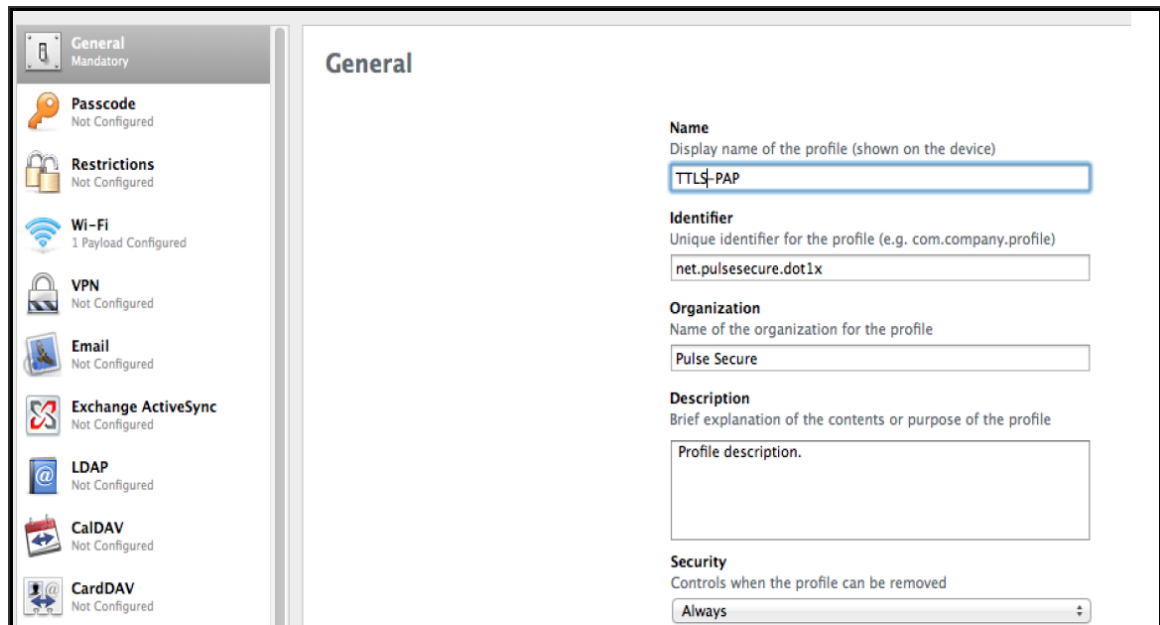
You can create various profiles (TTLS/PAP, TTLS/MS-CHAP-V2, and PEAP/MS-CHAP-V2) required for IPS 802.1x authentication using Apple Configurator. The generated configuration profiles can be exported to a Mac OSX endpoint. To create profiles, install the profiles (by double clicking on the exported files) on their OSX endpoints and that will provision Layer 2 access when connected to 802.1x enabled switch port.

Configuring 802.1x profiles -TTLS/PAP, TTLS/MS-CHAP-V2, and PEAP/MS-CHAP-V2 applies only for General and Wi-Fi settings. If the authentication server is LDAP, use TTLS-PAP for LDAP servers. If the authentication server is Active Directory or local, use TTLS-MSChapV2 or PEAP-MSChapV2.

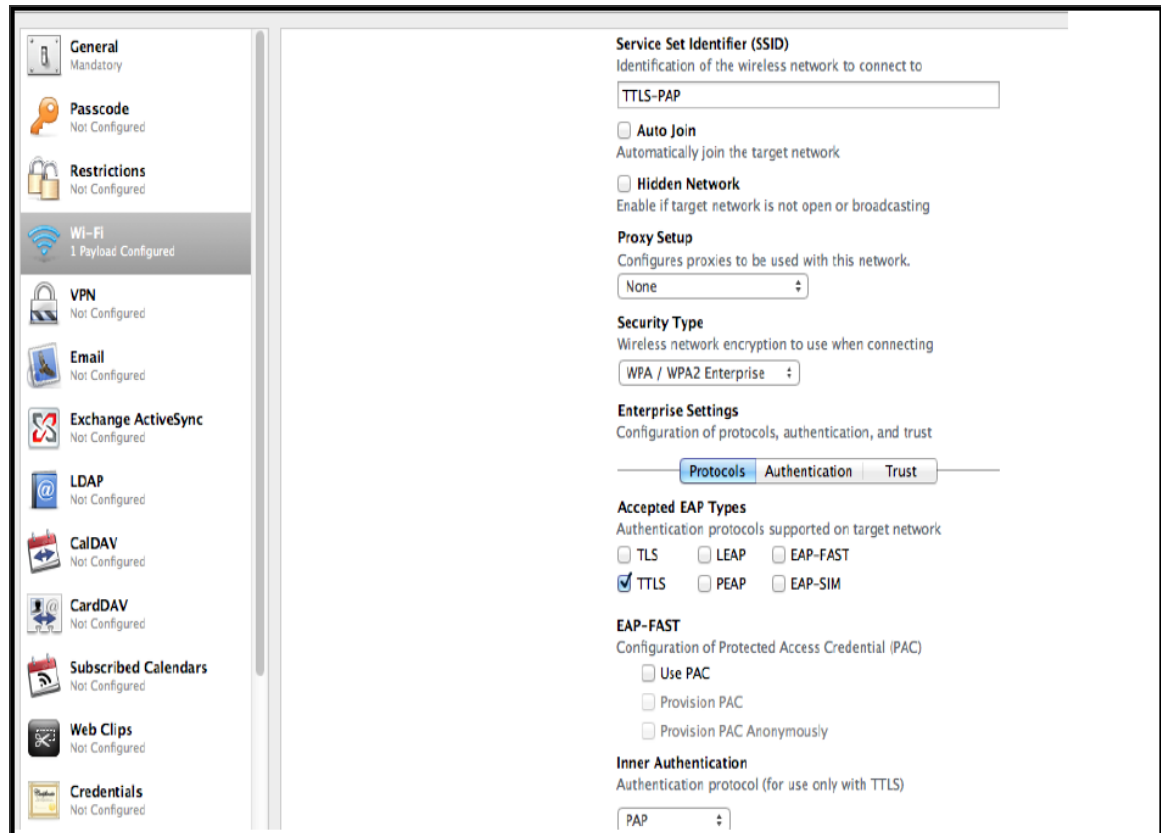
Configuring TTLS-PAP Authentication Profile

To configure TTLS-PAP profile, perform the following:

1. On the iPhone configuration utility (IPCU) navigate to **Configuration Profiles** tab.
2. On configuration Profiles page, select General and enter the required values.



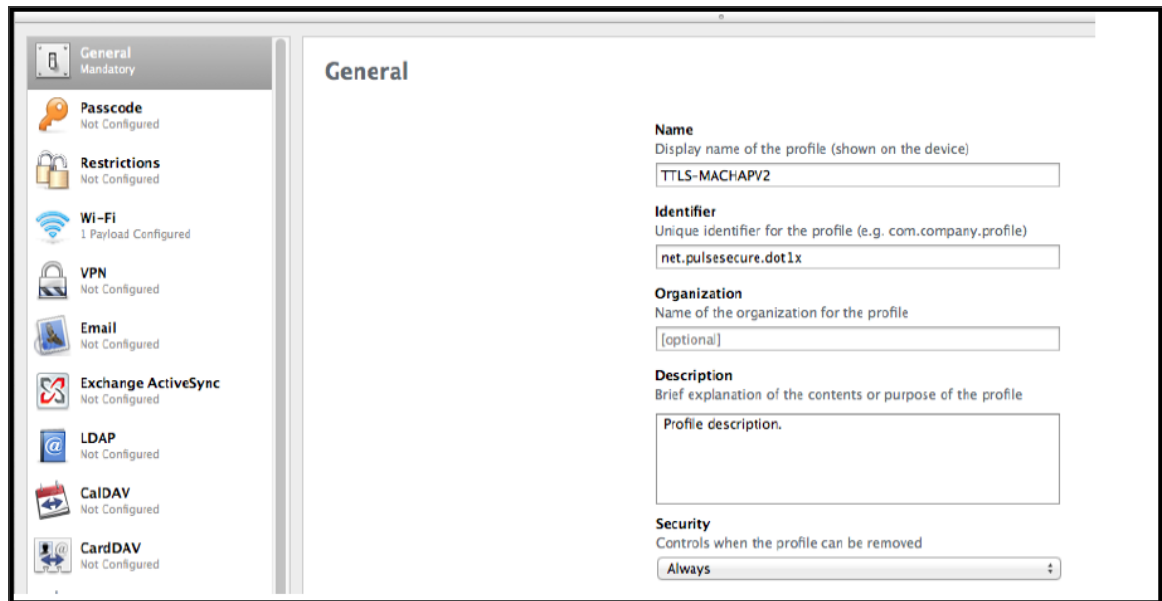
3. Select Wi-Fi and enter the required values.



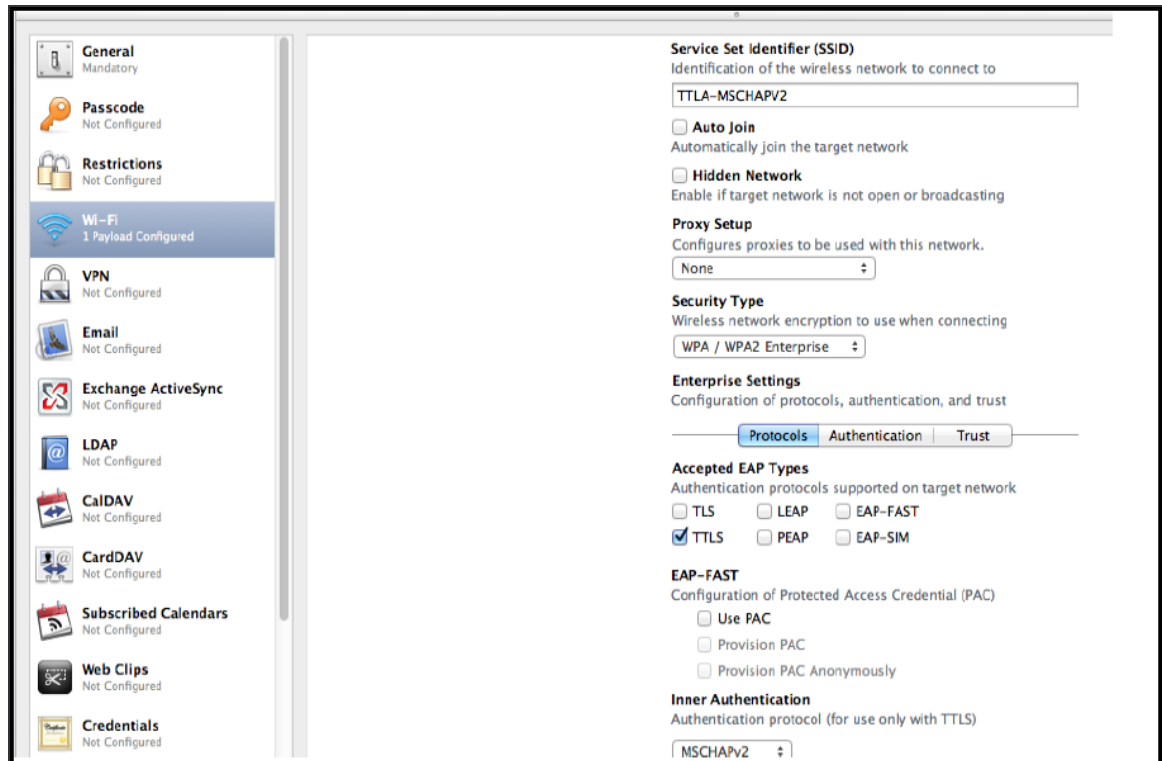
Configuring TTLS/MS-CHAP-V2 Authentication Profile

To configure TTLS/MS-CHAP-V2, perform the following:

1. On the iPhone configuration utility (IPCU) navigate to **Configuration Profiles** tab.
2. On configuration Profiles page, select General and enter the required values.



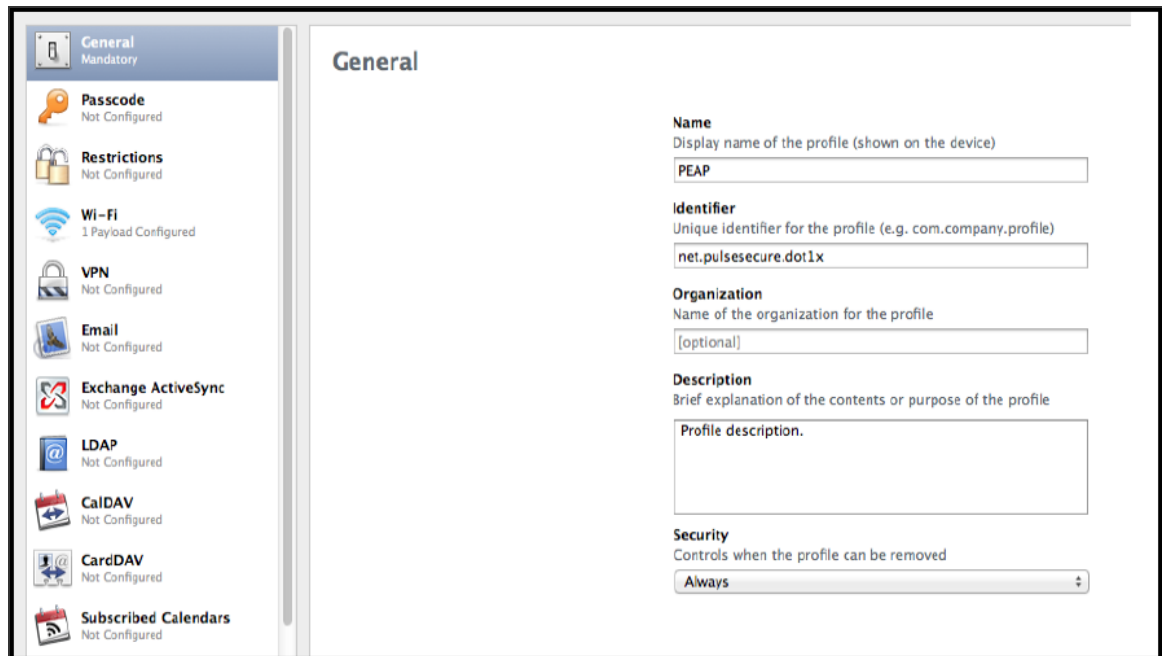
3. Select **Wi-Fi** and enter the required values.



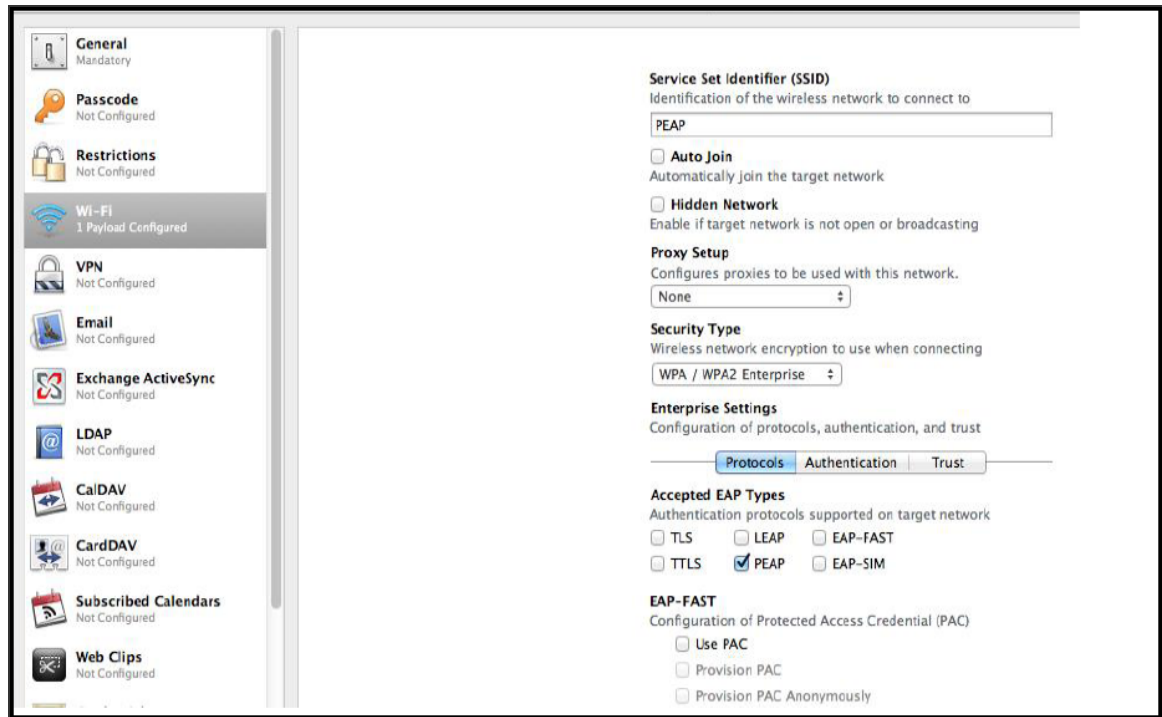
Configuring PEAP Authentication Profile

To configure PEAP, perform the following:

1. On the iPhone configuration utility (IPCU) navigate to **Configuration Profiles** tab.
2. On configuration Profiles page, select **General** and enter the required values.



3. Select **Wi-Fi** and enter the required values.



Layer 3 Enforcement

Layer 3 enforcement means using devices other than L2 switches or wireless access points for enforcement. This includes adding SRX, ScreenOS, Palo Alto, Fortigate, and Check Point firewall as enforcement points.

Enforcement using Check Point Next-Generation Firewall

Overview

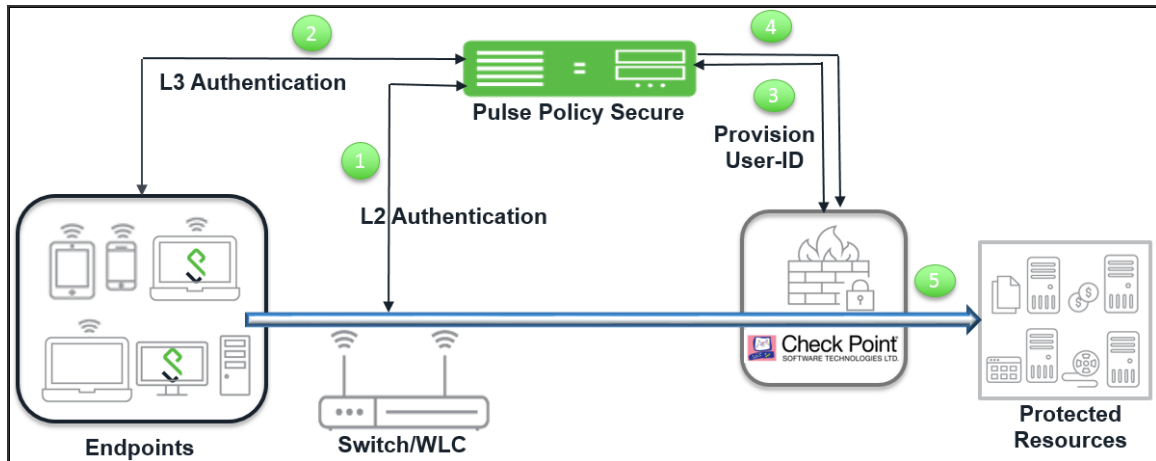
IPS delivers layer 3 network access control solution when deployed with Check Point Next-Generation Firewall (NGFW). IPS authenticates users, ensures that the endpoints meet security policies, and then dynamically updates the firewall enforcement point with the resulting user session information. Upon successful user authentication with IPS, the access to protected resources behind the firewall is based on the user identity, IP address, and user role information provided by IPS.

The IPS and Check Point firewall integration provides identity enabled layer 3 enforcement for BYOD, guests, and enterprise employees and protects corporate sensitive data from unauthenticated access and attacks.

Deployment of IPS using Check Point Next-Generation Firewall

This section describes the integration of IPS with Check Point Next-Generation Firewall. The Check Point Next-Generation Firewall controls the access to resources (for example, internet, CRM systems, Wikis and so on.) based on policy settings that defines the access. The Check Point Next-Generation Firewall allows integration with directory sources (For example, AD or LDAP) to get user and group information. The policies are then defined based on user role information.

IPS serves as the provider of identity information (For example, user-ID, IP address, and roles) for Check Point Next-Generation Firewall. The Check Point Next-Generation Firewall uses the identity information provided by the IPS for deciding the resource access.



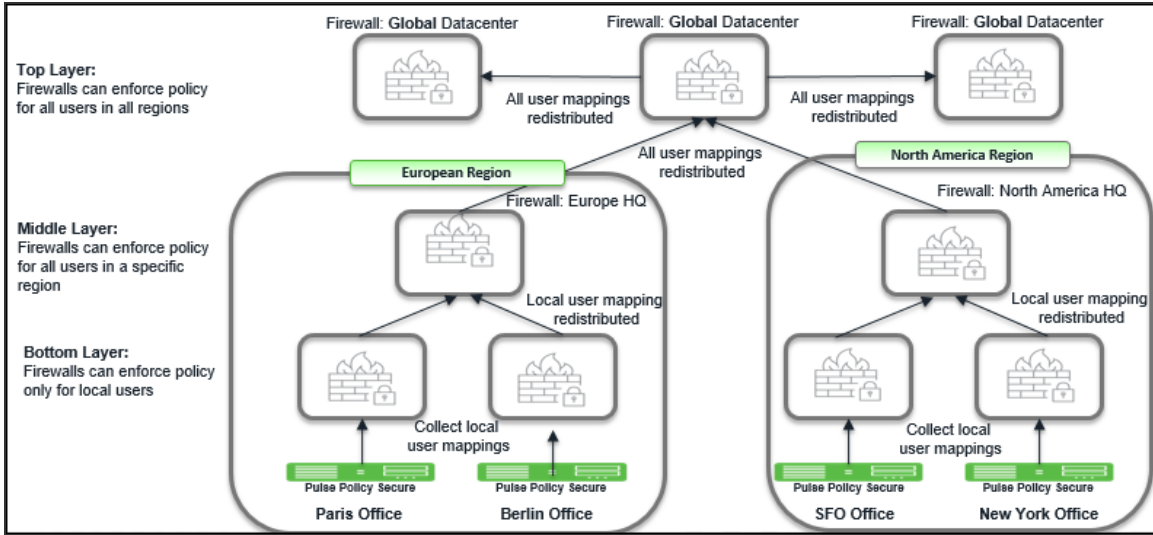
The authentication process is described below:

1. The endpoints connect to Switch/WLAN and performs the layer 2 authentication with IPS.
2. IPS performs the layer 3 authentication and performs compliance check on the endpoint and detects for any unauthorized behavior. IPS can also learn endpoint IP address using accounting and provision mapping.
3. IPS provisions the auth table entries (user-ID, IP address, and roles) on the Check Point Next-Generation Firewall.
4. The user role changes, which includes any unauthorized behavior are dynamically updated on the firewall. IPS provisions the auth table with changes in role information if any on Check Point Next-Generation Firewall. The access is based on roles.
5. The Check Point Next-Generation Firewall applies policies to allow or block user access to protected resources.

Deployment of IPS with Check Point Next-Generation Firewall for a Large Enterprise

For an enterprise with remote branch offices connected to the headquarters with VPN, deploy the Security Gateway at the remote branch offices. When you enable Identity Awareness on the branch office Security Gateway, users are authenticated before they reach internal resources. The identity data on the branch office Security Gateway is shared with other Security Gateways to avoid unnecessary authentication.

For more information see, [Identity Awareness](#) feature of Check Point.



Configuring IPS with Check Point Next-Generation Firewall

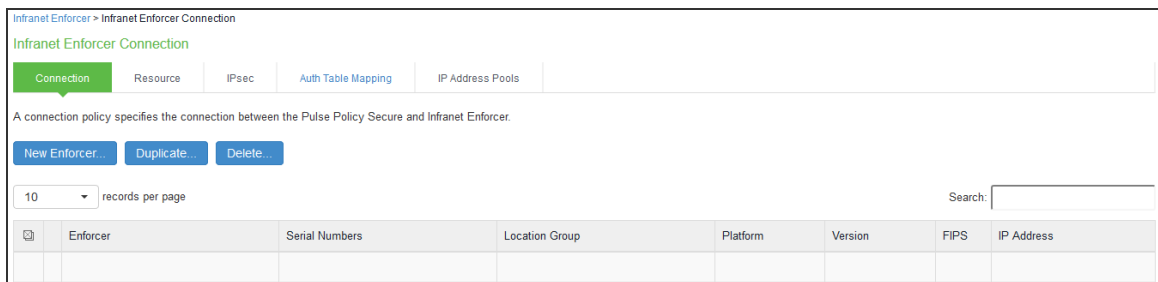
This section covers the configuration of IPS for adding Check Point Next-Generation Firewall as an Infranet Enforcer.

Configuring Check Point Infranet Enforcer in IPS

The IPS configuration requires defining a new Check Point Infranet Enforcer instance on IPS and then fetching the pre-configured shared secret key from the firewall. The shared secret key is used to communicate between the Check Point firewall and IPS. The standard user authentication / authorization configurations such as Auth Table Mapping Policies should also be created and associated with the required roles.

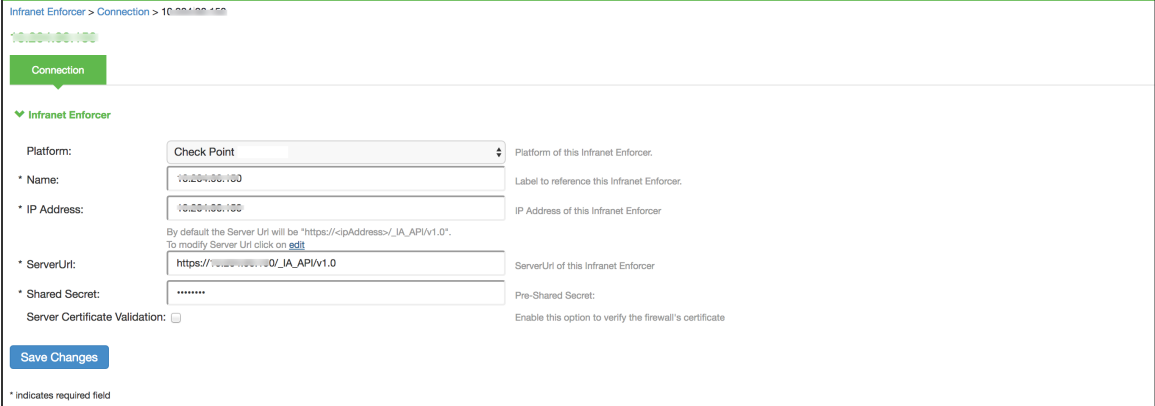
To configure a Check Point Firewall Infranet Enforcer in IPS:

1. Select **Endpoint Policy > Infranet Enforcer**.



2. Click **New Infranet Enforcer** and select **Check Point Firewall** in the **Platform** drop down.
3. Enter the Name and IP Address of the Check Point Next-Generation Firewall and enter the shared secret between IPS and Check Point.

 IPS has the default server URL for Check Point R80.10.



Infranet Enforcer > Connection > 10.001.001.000

Connection

Infranet Enforcer

Platform: Platform of this Infranet Enforcer.

* Name: Label to reference this Infranet Enforcer.

* IP Address: IP Address of this Infranet Enforcer

* ServerUrl: ServerUrl of this Infranet Enforcer
By default the Server Uri will be "https://<ipAddress>/_IA_API/v1.0". To modify Server Uri click on [edit](#).

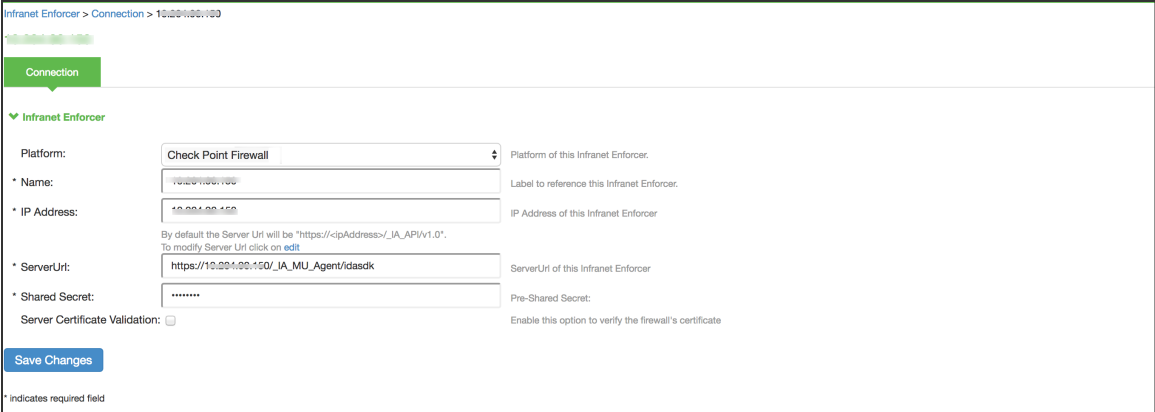
* Shared Secret: Pre-Shared Secret:

Server Certificate Validation: Enable this option to verify the firewall's certificate

[Save Changes](#)

* Indicates required field

For previous version of Check Point (R77.30), edit the server URL manually to `https://<IP_Address>/_IA_MU_Agent/idasdk`



Infranet Enforcer > Connection > 10.001.001.000

Connection

Infranet Enforcer

Platform: Platform of this Infranet Enforcer.

* Name: Label to reference this Infranet Enforcer.

* IP Address: IP Address of this Infranet Enforcer

* ServerUrl: ServerUrl of this Infranet Enforcer
By default the Server Uri will be "https://<ipAddress>/_IA_API/v1.0". To modify Server Uri click on [edit](#).

* Shared Secret: Pre-Shared Secret:

Server Certificate Validation: Enable this option to verify the firewall's certificate

[Save Changes](#)

* Indicates required field

4. (Optional) Select **Server Certificate Validation** to verify the firewall certificate.
5. Click **Save Changes**.

Configuring Auth Table Mapping Policies

An auth table entry consists of the user's name, a set of roles, and the IP address of the user device. An auth table mapping policy specifies which enforcer device (Firewall) can be used for each user role. These policies prevent the IPS from creating unnecessary auth table entries on all connected enforcer devices.

IPS's default configuration includes only one default auth table mapping policy. When the default auth table mapping policy is enabled, IPS pushes one auth table entry for each authenticated user to the selected Check Point Next-Generation Firewall configured as Infranet Enforcers in IPS.

To configure an Auth Table Mapping Policy:

1. Select **Endpoint Policy > Infranet Enforcer > Auth Table Mapping** and click **New Policy**.

Infranet Enforcer > Infranet Enforcer Auth Table Mapping Policies > New Policy

New Policy

* Name:

Description:

▼ Infranet Enforcer

Specify the Infranet Enforcer(s) to which this policy applies.

Available Enforcers:

Selected Enforcers:

▼ Roles

Policy applies to ALL roles
 Policy applies to SELECTED roles
 Policy applies to all roles OTHER THAN those selected below

Available roles:

Selected roles:

▼ Actions

Always Provision Auth Table
 Provision Auth Table As Needed Only available for Juniper enforcers.
 Never Provision Auth Table

VSYS:

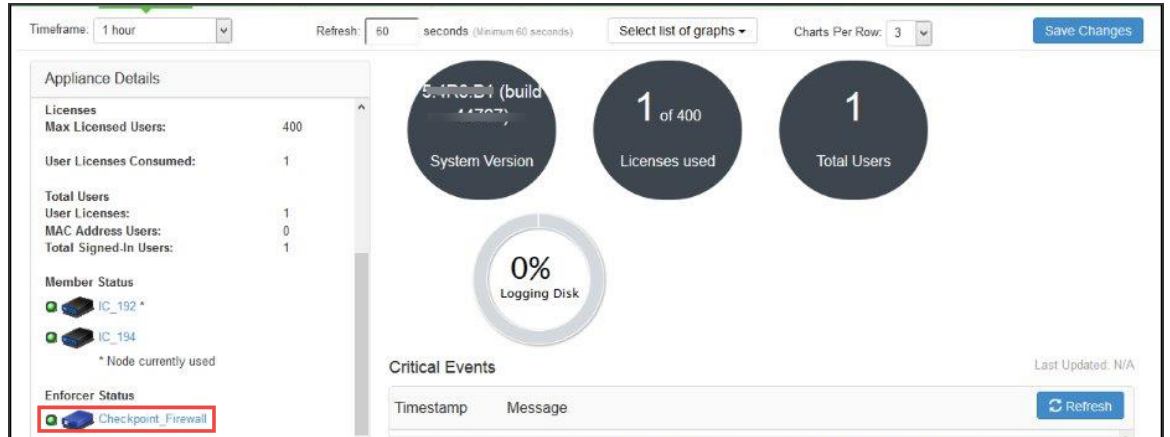
▼ One-to-one NAT Deployment

Provision Auth table for one-to-one NAT Deployment Enable this option to provision Auth Table for one-to-one NAT Deployment

* indicates required field

2. On the New Policy page:
 1. For Name, enter a name to label the auth table mapping policy.
 2. (Optional) For Description, enter a description.
 3. In the Enforcer section, specify the Infranet Enforcer firewall(s) to which you want to apply the auth table mapping policy.
 4. In the Roles section, specify:
 - Policy applies to ALL roles-Select this option to apply the auth table mapping policy to all users.
 - Policy applies to SELECTED roles-Select this option to apply the auth table mapping policy only to users who are mapped to roles in the SELECTED roles list. You can add roles to this list from the available roles list.
 - Policy applies to all roles OTHER THAN those selected below-Select this option to apply the auth table mapping policy to all users except for those who map to the roles in the SELECTED roles list. You can add roles to this list from the available roles list.
 5. In the Action section, specify auth table mapping rules for the specified Infranet Enforcer.
 - Always Provision Auth Table-Select this option to automatically provision auth table entries for chosen roles on the specified Infranet Enforcer.
 - Provision Auth Table as Needed-Select this option to provision auth table entries only when a user with a chosen role attempts to access a resource behind the specified Infranet Enforcer. This option is greyed out for Check Point Firewall Enforcers since it is not supported.
 - Never Provision Auth Table-Select this option to prevent chosen roles from accessing resources behind the specified Infranet Enforcer.
 6. You must delete the Default Policy if you configure any custom auth table mapping policies. IPS's default configuration includes this default auth table mapping policy that allows all source IP endpoints to use all Infranet Enforcers.

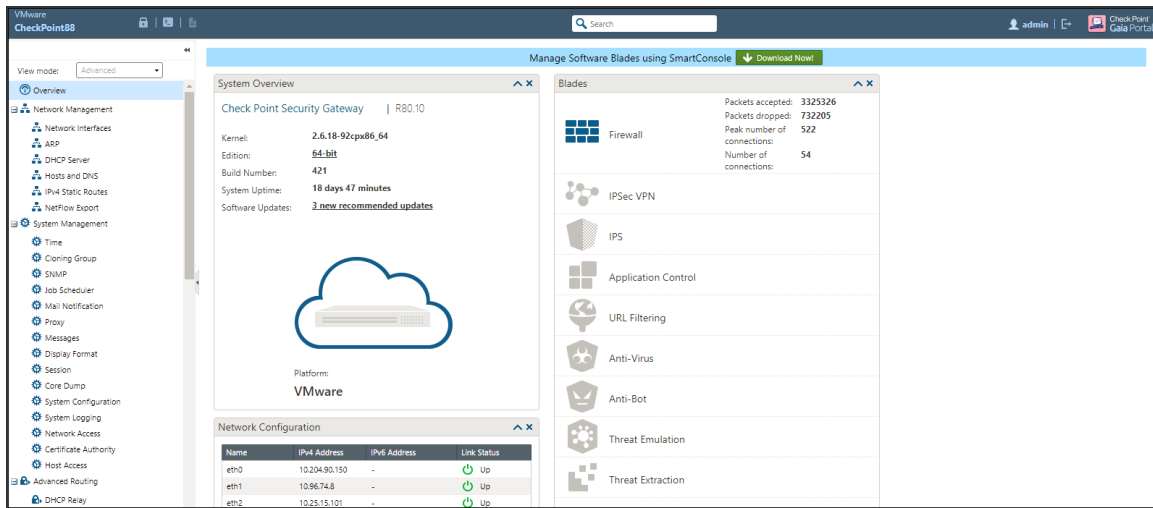
7. Click **Save Changes**.



Configuring Check Point Next-Generation Firewall

Check Point firewall detects traffic from an endpoint that matches a configured security policy using the access roles. It determines the role(s) associated with that user, and allows or denies the traffic based on the actions configured in the security policy.

The network interfaces are configured on the Check Point Next-Generation firewall and the remaining configurations are done on the Check Point Smart Console.

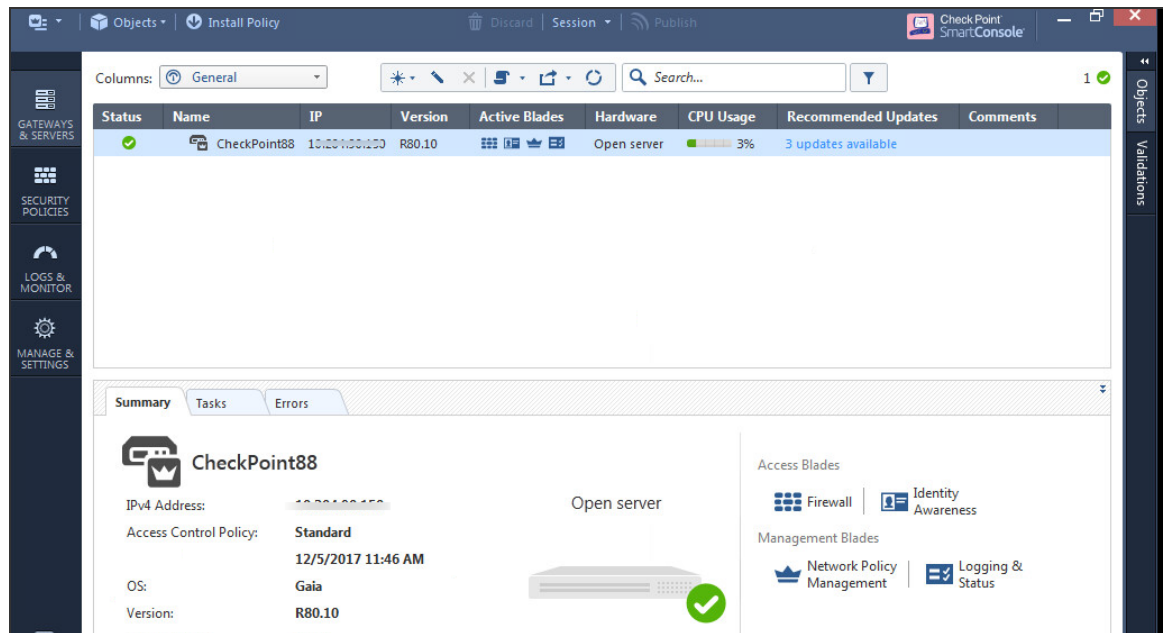


Configuring Identity Awareness in SmartConsole

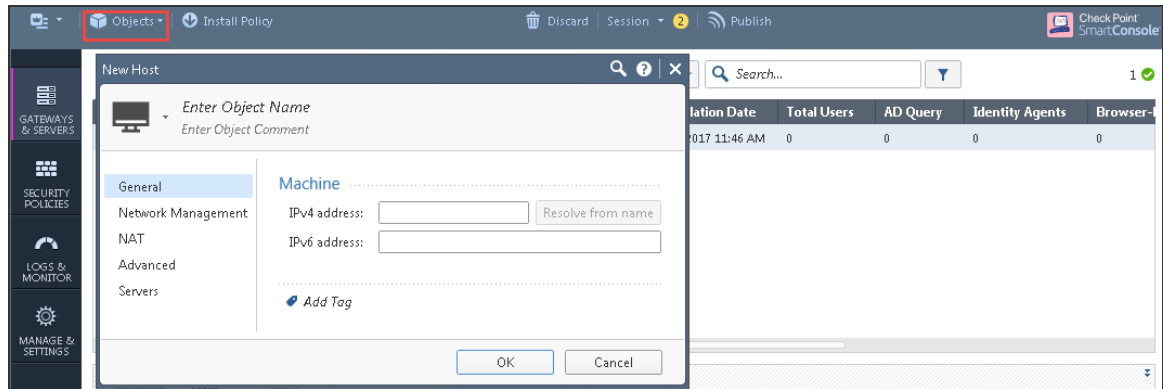
The Identity Awareness lets you easily configure network access and auditing based on network location, identity of user, and identity of the device. When Identity Awareness identifies a source or destination, it shows the IP address of the user or computer with a name. For example, this lets you create firewall rules with any of these properties. You can define a firewall rule for specific users when they send traffic from specific computers or a firewall rule for a specific user regardless of which computer they send traffic from.

To enable Identity awareness:

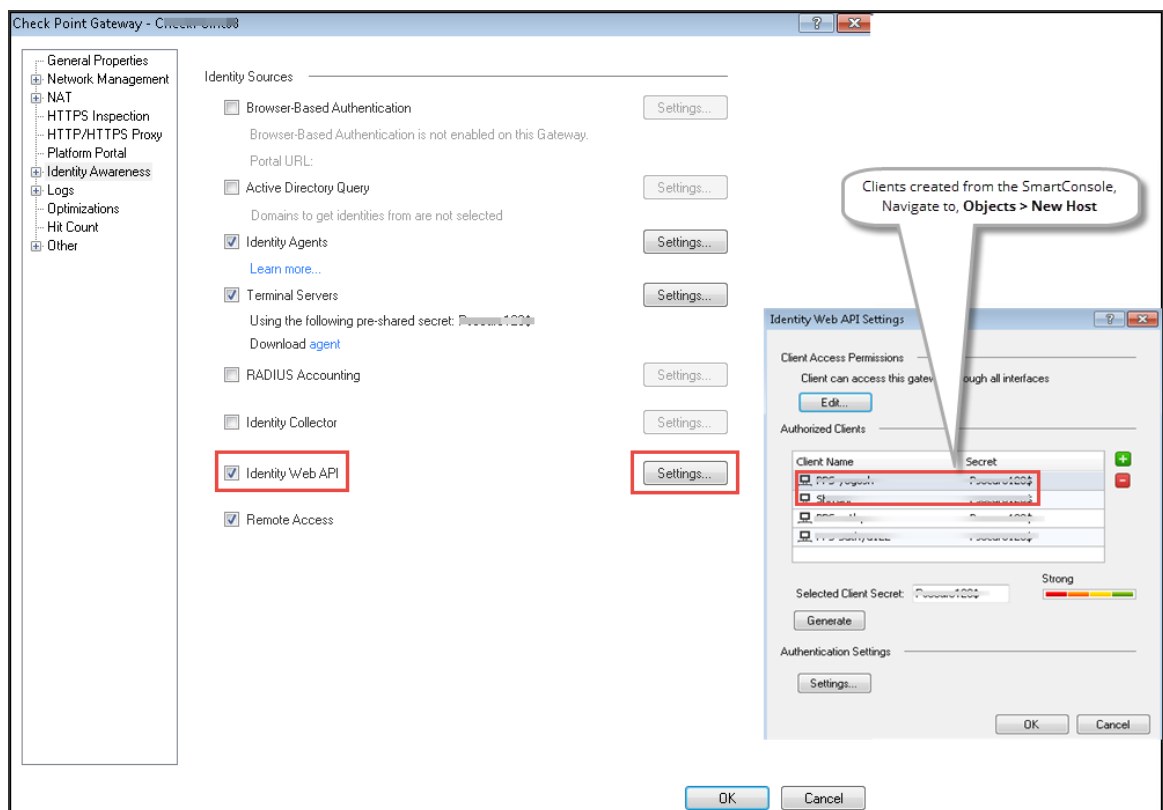
1. Login to the Check Point SmartConsole.
2. From the **Security & Gateways view**, double-click the Security Gateway on which to enable identity awareness.




3. Create an object for IPS. Select **Objects > New Host** and enter the IPS IP address. Under Servers, enable Web Server and click **OK**.

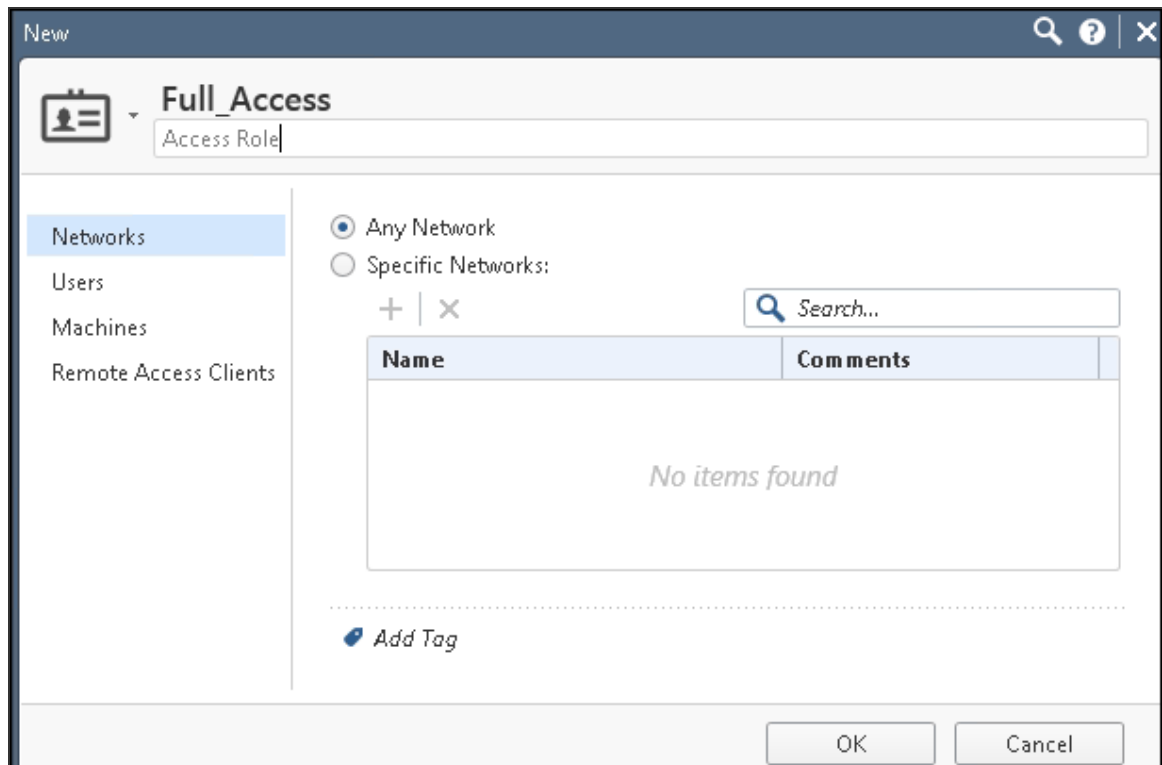


4. Select **Gateways & Servers > Identity Awareness** and enable the following options:
 - **Terminal Servers**- Note down the pre-shared secret key.
 - **Identity Web API**- Click **Settings** and add the IPS device as Authorized Clients.

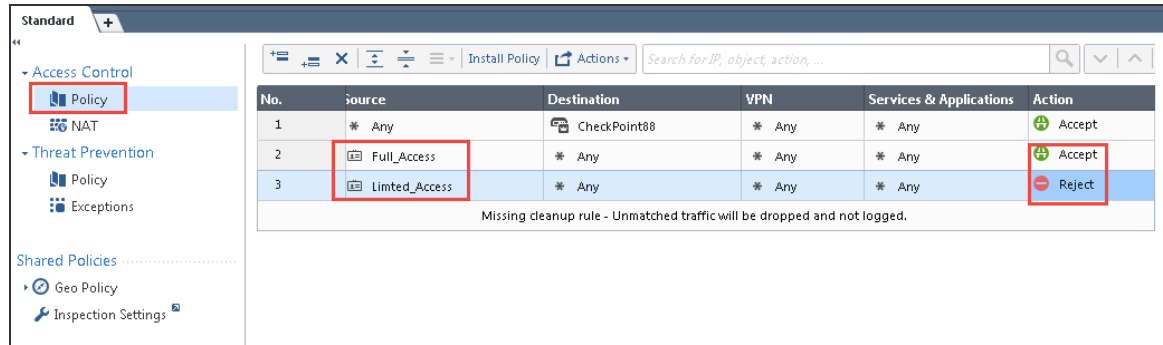


5. Click **Install Policy**.
6. From the Object Explorer create an object for Identity matching by creating user roles. Select Objects > Object Explorer and Click **New > Users > Access Role**.

 The role names must match with the Role names created on IPS.



- From the SmartConsole, create a security policy by keeping the Access Role in Source column. Select **Security Policies > Access Control > Policy** and then configure the required policies. For example, Full_Access policy allows traffic from Client with Full_Access role, Limited_Access role policy denies traffic from Client with Limited_Access role, and default_allow policy which allows all traffic. The Full_Access role is on the top of the list since it should be considered first.



- Click **Install Policy**.

Troubleshooting

You can use the following CLI commands (Expert Mode) on the Check Point firewall for troubleshooting:

- `pdp monitor all` - Displays the table of user identities mapped to IP addresses.

Unsupported Features

The following features are not supported:

- IP Address Pools
- IPsec Enforcement
- IDP Sensors
- Virtual Systems (VSYS)
- Enforcement for endpoints behind Network Address Translation (NAT)
- Resource access policies. The administrator should configure all firewall policies on the firewall through smartboard

Enforcement using Palo Alto Networks Firewall

Overview

IPS delivers layer 3 network access control solution when deployed with Palo Alto Networks next-generation firewalls. IPS authenticates users, ensures that the endpoints meet security policies, and then dynamically updates the firewall enforcement point with the resulting user session information. Upon successful user authentication with IPS, the access to protected resources behind the firewall is based on the user identity, IP address, and user role information provided by IPS.

The IPS and PAN integration provides identity enabled layer 3 enforcement for BYOD and guests as well as enterprise employees, with the end authentication and comprehensive compliance checks from IPS.

Deployment of IPS using PAN Firewall

This section describes the integration of IPS with Palo Alto Networks next-generation firewall. The IPS and PAN firewall integration allows users to enforce role based access to network resources and web applications and ensures endpoint compliance. The integrated solution provides policy enforcement for end to end protection of sensitive corporate data from unauthenticated access and attacks.

IPS combines user identity and device security state information with network location to create a unique, session specific access control policy for each user. The Palo Alto Networks firewall provides a feature called User Identification (User-ID) that creates policies and performs reporting based on users and groups rather than individual IP addresses. IPS uses the User-ID XML API to send the IP address to user and IP address to Group (Role) mapping information to the Palo Alto Networks firewall. PAN firewall enables the flexibility to apply different rules to the same server based on tags. A tag is a metadata element, which defines its role on the network, the operating system, or the different kinds of traffic it processes.

The Palo Alto Networks firewall compares the user information against the tag that is associated to a security rule. If the User Role name matches the tag, then traffic is either allowed or denied based on the configuration. When a user logs in, Ivanti Policy Secure provisions their user ID, IP address of the endpoint, and role information to the Palo Alto Networks firewall; that enables firewall policies based on any of these attributes to be enforced.

Similarly, when a user logs out, the user ID, IP address of the endpoint, and role information is removed from the firewall. More importantly, when a user's role changes, the role change information is dynamically updated on the firewall, so that access based on the updated roles is automatically changed based on the policy matched by the new information.

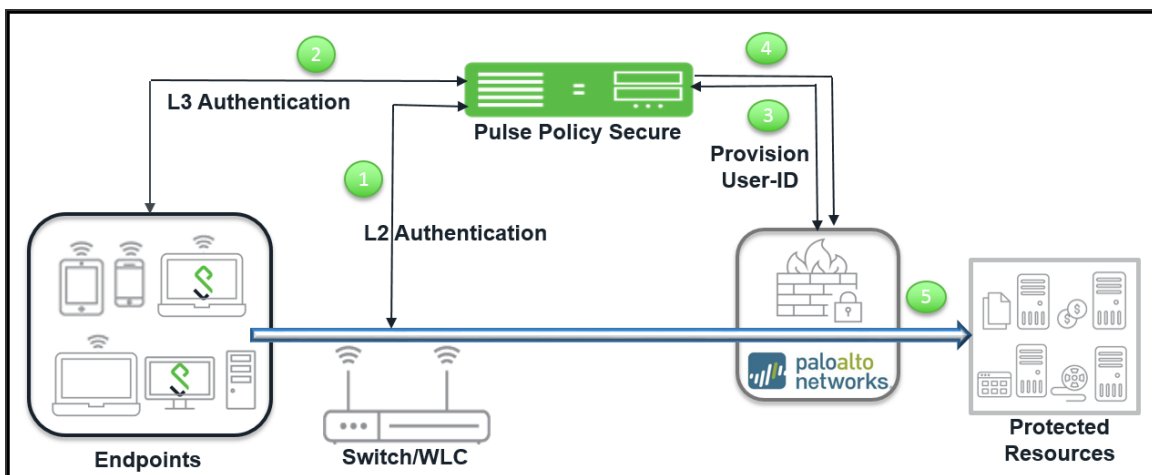
With Palo Alto Networks firewall integration, all users' role changes, which includes compliance check failure or unauthorized behavior are dynamically updated on the firewall. The access is based on user roles and not merely on source IP addresses.

IPS is the policy decision point that determines which users and endpoints can access protected resources. Palo Alto Networks Next Gen firewalls serve as the policy enforcement points to provide the ultimate protection to ensure that network assets are secured.

Palo Alto Networks integration with Ivanti Policy Secure leverages dynamic role information provisioned to the firewall upon user session establishment and for the duration of the session. Ivanti Policy Secure also communicates user information to the Palo Alto Networks firewall when users log in or log out from their device.

Deploying IPS with a PAN firewall for a Small Enterprise

IPS and PAN integration can be used for role based layer 3 access control. For small scale enterprise deployment, you can use a single IPS and PAN firewall as it involves less number of users. For example, employees, contractors, and guest users. A single IPS device provisioning to a PAN firewall can handle up to 30,000 user sessions. The following is a sample deployment with a IPS device along with a PAN firewall.

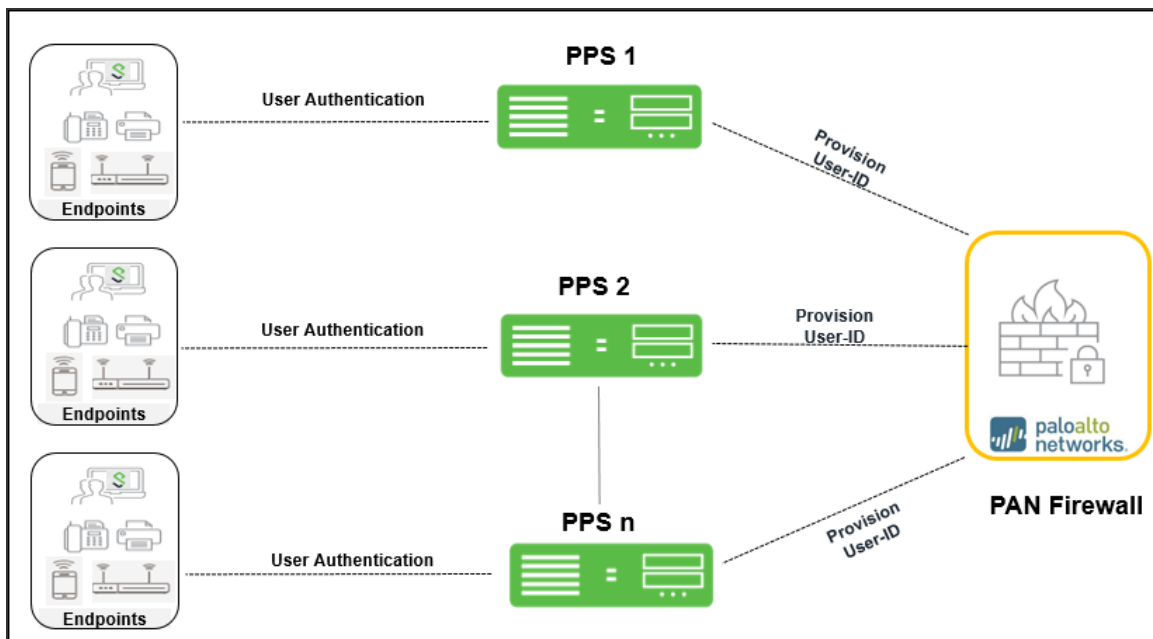


The authentication process is described below:

1. The endpoints connect to switch/WLAN and performs the layer 2 authentication with IPS.
2. IPS performs the layer 3 authentication and performs compliance check on the endpoint and detects for any unauthorized behavior.
3. IPS provisions the auth table entries on the PAN firewall.
4. IPS provisions the auth table with changes in role information if any on PAN firewall. The user role changes, which includes any unauthorized behavior are dynamically updated on the firewall. The access is based on roles, rather than only on source IP addresses.
5. The PAN firewall applies policies to allow or block user access to protected resources.

Deploying multiple IPS with PAN firewall

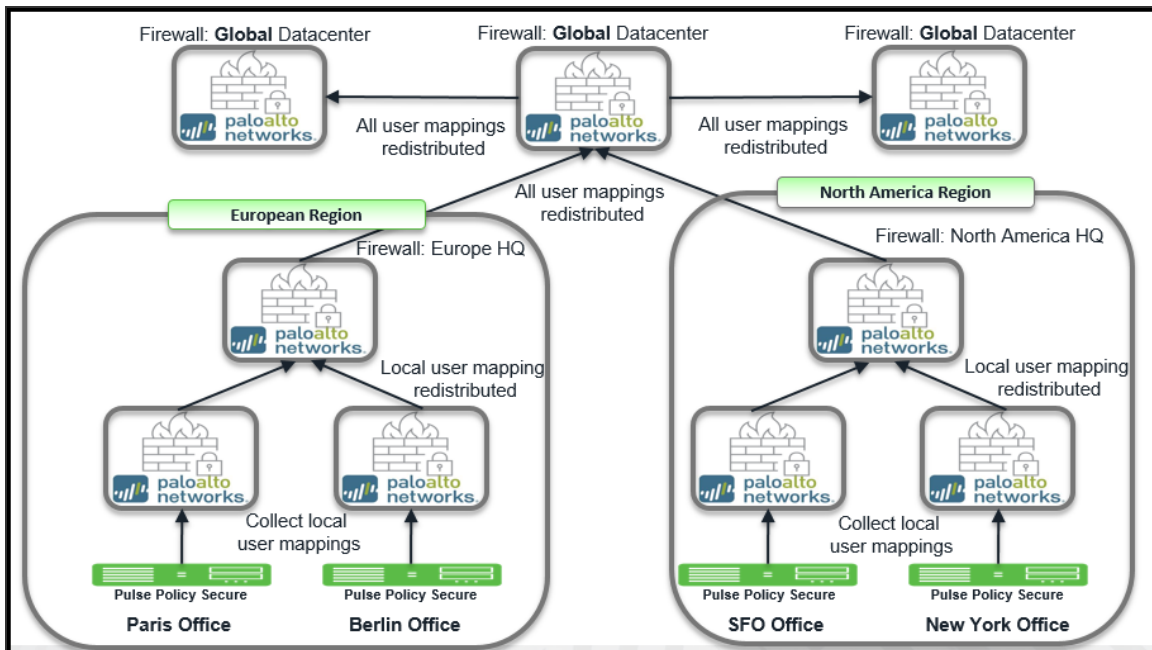
The deployment example describes an enterprise environment with multiple IPS servers where different users are authenticated using different IPS servers. For such deployments, multiple IPS servers can be configured to communicate with a single PAN firewall. The multiple IPS servers sends user-ID entries to a single PAN firewall.



Deploying IPS with PAN firewall for a Large Enterprise

A large-scale enterprise network uses multiple firewalls to enforce policies. You can reduce the resources that the firewalls and information sources use in the querying process by configuring some firewalls to acquire mapping information. You can enable the firewall to enforce user based policies when users rely on local sources for authentication (for example, regional directory services) but need access to remote resources (for example, global data center applications).

The deployment example describes how a global datacenter resources is distributed across the branches and shared across the local offices. It also shows how you can organize the redistribution sequence in layers, where each layer has one or more firewalls. In this example, bottom-layer firewalls in local offices rely on IPS for authentication and then redistribute the mapping information to middle-layer firewalls in regional offices, which redistribute to one top-layer firewall in a global data center. The data center firewall redistributes the mapping information to other data center firewalls so that they can enforce global policies for all users.



Specification for deploying IPS and PAN Appliances

The firewall provides access to resources based on the user role. You can use the IP role mapping on the PAN firewall for role based access. The maximum number of IP addresses that can be registered for each PAN device is different. The following table describes the specifics for different PAN firewall appliances and the recommended IPS appliance for your deployment.

PAN Appliance	Maximum number of dynamically registered IP addresses	IP Address Tag	Recommended IPS Appliance
PA 500	1,000	32	PSA 5000
PA3020	5,000	32	PSA 5000
PA 5020	20,000	32	SM 360, PSA 7000
PA 7000	44,000	32	PSA 7000

- The IP role mapping scale limit or the maximum number of dynamically registered IP addresses for a unique endpoint is based on the PAN appliance.

- The maximum number of IP address tags supported is also based on the PAN appliance.



- The IP Address tag is a metadata element or attribute-value pair that is registered on the firewall. For example, IP1 {tag1, tag2,.....tag32}, where the IP address and the associated tags are maintained as a list; each registered IP address can have up to 32 tags such as the operating system, the datacenter or the switch to which it belongs.

Configuring IPS with PAN Firewall

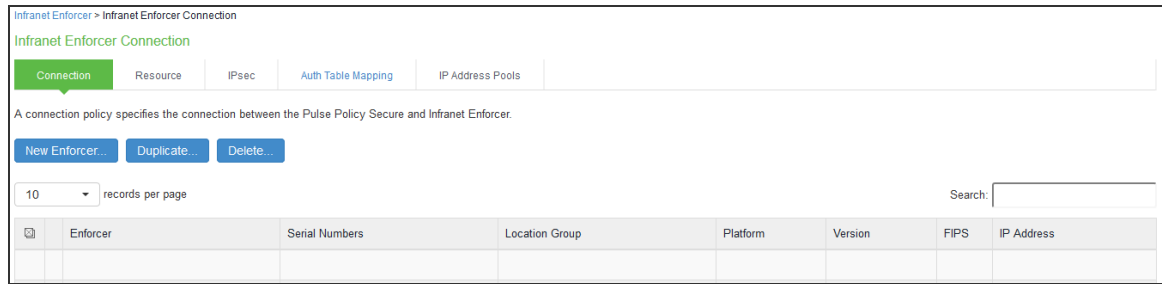
This section covers the configuration of IPS for adding PAN firewall as an Infranet Enforcer.

Configuring PAN Infranet Enforcer in IPS

The IPS configuration requires defining a new Palo Alto Networks Firewall Infranet Enforcer instance on IPS and then fetching the API key from the firewall. The API key is used to communicate between the Palo Alto Networks firewall and IPS. The standard user authentication / authorization configurations such as Auth Table Mapping Policies should also be created and associated with the required roles.

To configure a Palo Alto Networks Firewall Infranet Enforcer in IPS:

1. Select **Endpoint Policy > Infranet Enforcer**.



2. Click **New Infranet Enforcer** and select Palo Alto Networks Firewall in the Platform drop down.

3. Enter the **Name** and **IP Address** of the Palo Alto Networks firewall and then click **Get API Key** which opens a new page:

4. Enter the **Admin Username** and **Admin Password** of the Palo Alto Networks firewall and then Click **Retrieve**. This enables IPS to fetch the API key of the firewall. Once the API key is retrieved, the page automatically redirects back to the New Infranet Enforcer page as shown above and updates the API Key Field.
See Configuring PAN Device Certificates for understanding the validation procedure.
5. Click **Save Changes**.

Configuring Auth Table Mapping Policies

An auth table entry consists of the user's name, a set of roles, and the IP address of the wired, wireless, or virtual adapter. An auth table mapping policy specifies which enforcer device can be used for each user role. These policies prevent the IPS from creating unnecessary auth table entries on all connected enforcer devices.

IPS's default configuration includes only one default auth table mapping policy. When the default auth table mapping policy is enabled, IPS pushes one auth table entry for each authenticated user to all Palo Alto Networks firewalls configured as Infranet Enforcers in IPS.

To configure an Auth Table Mapping Policy:

1. Select **Endpoint Policy > Infranet Enforcer > Auth Table Mapping** and click **New Policy**.

Infranet Enforcer > Infranet Enforcer Auth Table Mapping Policies > AuthTablePolicy

AuthTablePolicy

General

* Name: AuthTablePolicy

Description: AuthTablePolicy

▼ Infranet Enforcer

Specify the Infranet Enforcer(s) to which this policy applies.

Available Enforcers: CHKPNT

Selected Enforcers: PAN

Add ->

Remove

▼ Enforcement Settings

Enable this option to provision only IP-User mapping to Palo Alto Networks Enforcer. Applicable to Palo Alto Networks Enforcer only.

Provision only IP-User mapping to Palo Alto Networks Enforcer

▼ Roles

Policy applies to ALL roles

Policy applies to SELECTED roles

Policy applies to all roles OTHER THAN those selected below

Available roles: Guest, Guest Admin, Guest Sponsor, Guest Wired Restricted

Selected roles: Users

Add ->

Remove

▼ Actions

Always Provision Auth Table

Provision Auth Table As Needed Only available for Juniper enforcers.

Never Provision Auth Table

VSYS: vsys2

▼ One-to-one NAT Deployment

Provision Auth table for one-to-one NAT Deployment Enable this option to provision Auth Table for one-to-one NAT Deployment.

Save Changes Save as Copy

2. On the New Policy page:

- For Name, enter a name to label the auth table mapping policy.
- (Optional) For Description, enter a description.
- In the Enforcer section, specify the Infranet Enforcer firewall(s) to which you want to apply the auth table mapping policy.
- Under Enforcement Settings, Admin can enable **Provision only IP-User mapping to Palo Alto Networks Enforcer** to provision only the IP-user mapping information to Palo Alto Networks firewall.



This option is available only with Palo Alto Networks Enforcer.

If you are using group lookup (LDAP group from AD server) in the Palo Alto Networks security policy then enable “Provisioning only IP-User information to Palo Alto Networks Enforcer” in Ivanti Policy Secure to control resource access.

- In the Roles section, specify:
 - Policy applies to ALL roles-Select this option to apply the auth table mapping policy to all users.
 - Policy applies to SELECTED roles-Select this option to apply the auth table mapping policy only to users who are mapped to roles in the SELECTED roles list. You can add roles to this list from the available roles list.
 - Policy applies to all roles OTHER THAN those selected below-Select this option to apply the auth table mapping policy to all users except for those who map to the roles in the SELECTED roles list. You can add roles to this list from the available roles list.

- In the Action section, specify auth table mapping rules for the specified Infranet Enforcer.
 - Always Provision Auth Table-Select this option to automatically provision auth table entries for chosen roles on the specified Infranet Enforcer.
 - Provision Auth Table as Needed-Select this option to provision auth table entries only when a user with a chosen role attempts to access a resource behind the specified Infranet Enforcer. This option is greyed out for Palo Alto Networks Firewall Enforcers since it is not supported.
 - Never Provision Auth Table-Select this option to prevent chosen roles from accessing resources behind the specified Infranet Enforcer.
- 3. You must delete the Default Policy if you configure any custom auth table mapping policies. IPS's default configuration includes this default auth table mapping policy that allows all source IP endpoints to use all Infranet Enforcers.
- 4. If you created a vsys on a PAN Enforcer, enter the ID of the vsys in the vsys text box. To view the enforcers or vsys that are associated with each policy, select **Endpoint Policy > Infranet Enforcer > Auth Table Mapping**. If no VSYS ID is provided in VSYS textbox, then auth table will be provisioned to default VSYS in PAN firewall.
- 5. Enable **Provision Auth Table for one-to-one NAT deployment** to provision auth table entries for endpoints behind one-to-one NAT deployment. On enabling checkbox for "Provision Auth Table for one-to-one NAT deployment", admin will be redirected to a confirmation page. Click Enable button to enable the setting.
- 6. Click **Save Changes**.

Configuring Resource Access Policy

A resource access policy specifies which users are allowed or denied access to a set of protected resources. You can specify which users you want to allow or deny by choosing the roles for each resource access policy.

Resource Access Policy and IoT Policy Provisioning with Palo Alto Network's Firewall works only with default device name localhost.localdomain configuration.

Each Resource Access Policy is configured with single VSYS information. For a selected PAN firewall if resource access policy needs to be pushed to multiple VSYS, multiple Resource Access Policy need to be created that is one policy for each VSYS.

To configure Infranet Enforcer resource access policies:

1. Select **Endpoint Policy > Infranet Enforcer > Resource Access Policy** and **click New Policy**.

The screenshot shows the configuration page for a new Resource Access Policy named 'policy-vsyz2'. The page is divided into several sections:

- General:** The Name field is set to 'policy-vsyz2'. There is a note: 'Required: Label to reference this policy.' The Description field is empty.
- Infranet Enforcer:** The Platform is set to 'Palo Alto Networks Firewall'. Below this, there are two lists: 'Available Enforcers' (currently empty) and 'Selected Enforcers' (containing 'enf_pan (PANNGFW)'). There are 'Add ->' and 'Remove' buttons between the lists.
- Security Zones:** The Source Zone is set to 'untrust' and the Destination Zone is set to 'trust'. A note says: 'Specify firewall security zones for this policy. If security zone is not specified, then it applies to all zones i.e. any. Multiple zones can be specified with comma separated. Example: trust,mgmt'.
- Service:** The Service is set to 'any'.
- Resources:** The Resources field contains '10.25.15.85'. A note says: 'Specify the resources for which this policy applies, one per line.' Examples provided are: 'Enter an IP address or Subnet or IP address range', '192.168.80.150', '192.168.80.0/24', and '10.0.0.0-10.255.255.255'.
- Roles:** There are three radio button options: 'Policy applies to ALL roles', 'Policy applies to SELECTED roles' (which is selected), and 'Policy applies to all roles OTHER THAN those selected below'. Below are two lists: 'Available roles' (Guest, Guest Admin, Guest Sponsor, Guest Wired Restricted) and 'Selected roles' (Users). There are 'Add ->' and 'Remove' buttons between the lists.
- Actions:** There are two radio button options: 'Allow access' (which is selected) and 'Deny access'.
- Enforcer Options:** The VSYS field is set to 'vsyz1'.

At the bottom, there is a note: 'NOTE: changes to this page will cause a slight interruption of service for Infranet Enforcer Resource Policies users.' Below this are 'Save Changes' and 'Save as Copy' buttons. A small asterisk at the bottom left indicates required fields.

2. On the New Policy page:

- For Name, enter a name to label this Infranet Enforcer resource access policy.
- (Optional) For Description, enter a description.

For **Resources**, specify the protocol, IP address, network mask, and port of each resource (or range of addresses) for which this Infranet Enforcer resource access policy applies, one per line. Do not insert any spaces in your entries, or the policy may not be applied correctly.

You cannot specify a host name in a resource access policy. You can specify only an IP address. You can use TCP, UDP, or ICMP.

- Under Infranet Enforcer, specify the Infranet Enforcer to which this policy applies by using Add.
- Specify one of the following in the Roles section:
 - **Policy applies to ALL roles**-To apply this Infranet Enforcer resource access policy to all users.
 - **Policy applies to SELECTED roles**-To apply this Infranet Enforcer resource access policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
 - **Policy applies to all roles other than those selected below**- To apply this Infranet Enforcer resource access policy to all users except those who map to the roles in the Selected roles list. You must add roles to this list from the Available roles list.
- In the Action section, specify whether you want to use this Infranet Enforcer resource access policy to allow or deny access to the specified resources.
- If you have created a vsys on PAN Enforcer, enter the ID of the vsys in the VSYS text box, if applicable.

If no VSYS ID is provided in VSYS textbox, then policy will be pushed to default VSYS in PAN firewall.

The Infranet Enforcer > Resource Access Policy page displays the Enforcers and/or vsys that are associated with each policy.

	Policies	Action	Resources	Enforcer	Vsys	Applies to role
1.	policy-vsys2	Allow	10.10.10.10	ent_pan	vsys1	Users
2.	policy-vsys1	Allow	10.10.10.05	ent_pan	vsys1	Users
3.	rap1	Allow	1.1.1.1	ent_pan		All roles

Configuring Palo Alto Networks Firewall

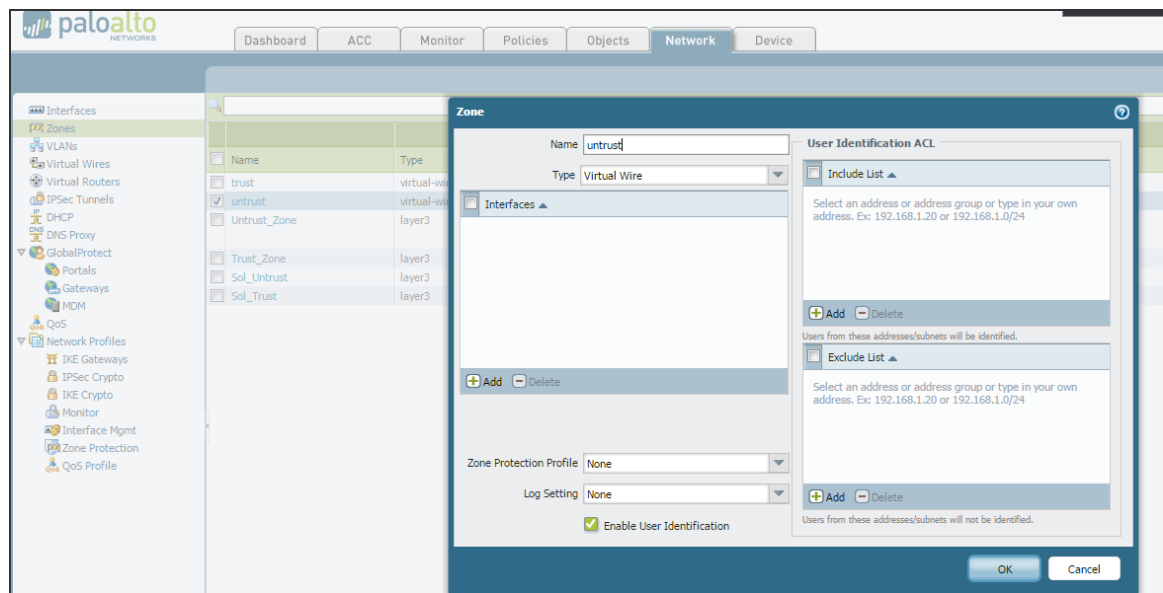
Palo Alto Networks firewall detects traffic from an endpoint that matches a configured security policy using the endpoint's auth table entry. It determines the role(s) associated with that user and allows or denies the traffic based on the actions configured in the security policy.

Configuring User Identification on Security Zones

Policy rules on the firewall use security zones to identify the source and the destination of the traffic. The data traffic flows freely within a zone and not between different zones until you define a security policy rule that allows it. To enable User-ID enforcement, you must enable User Identification on both inbound and outbound zones traversed by the end-user traffic.

To enable User Identification:

1. Select **Palo Alto Networks > Network > Zones**.
2. For each zone that serves as an inbound or outbound zone for enforced traffic, click the zone name (For example, trust, untrust, and so on).
3. Select **Enable User Identification** and click **OK**.



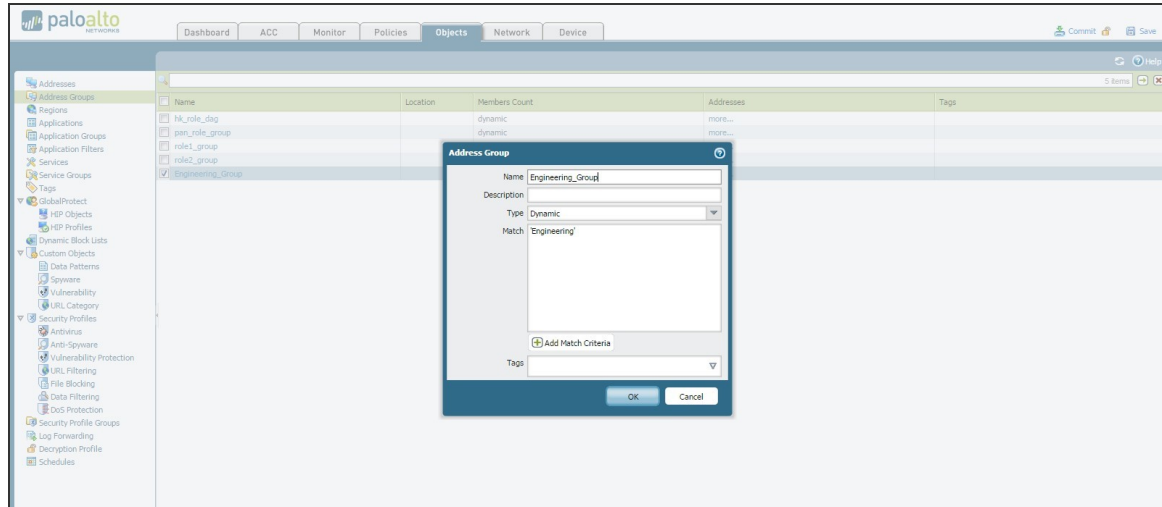
Provisioning of Resource Access Policies from IPS to the Palo Alto Networks Firewall Enforcer is not supported. You must configure the required security policies on the firewall.

Configuring Dynamic Address Groups

Dynamic address groups allow you to create policy that automatically adapts to changes-adds, moves, or deletions of servers. It also enables the flexibility to apply different rules to the same server based on its role on the network or the different kinds of traffic it processes.

To configure a dynamic address group:

1. Select **Palo Alto Networks > Objects > Address Groups**.



2. Click **Add** and enter a Name and a Description for the address group.
3. Select Type as **Dynamic**. Define the match criteria. You can select dynamic and static tags as the match criteria to populate the members of the group.
4. Enter the role name of the users. The role name in the Match section should match the roles that are configured in IPS.
5. Click **OK**.



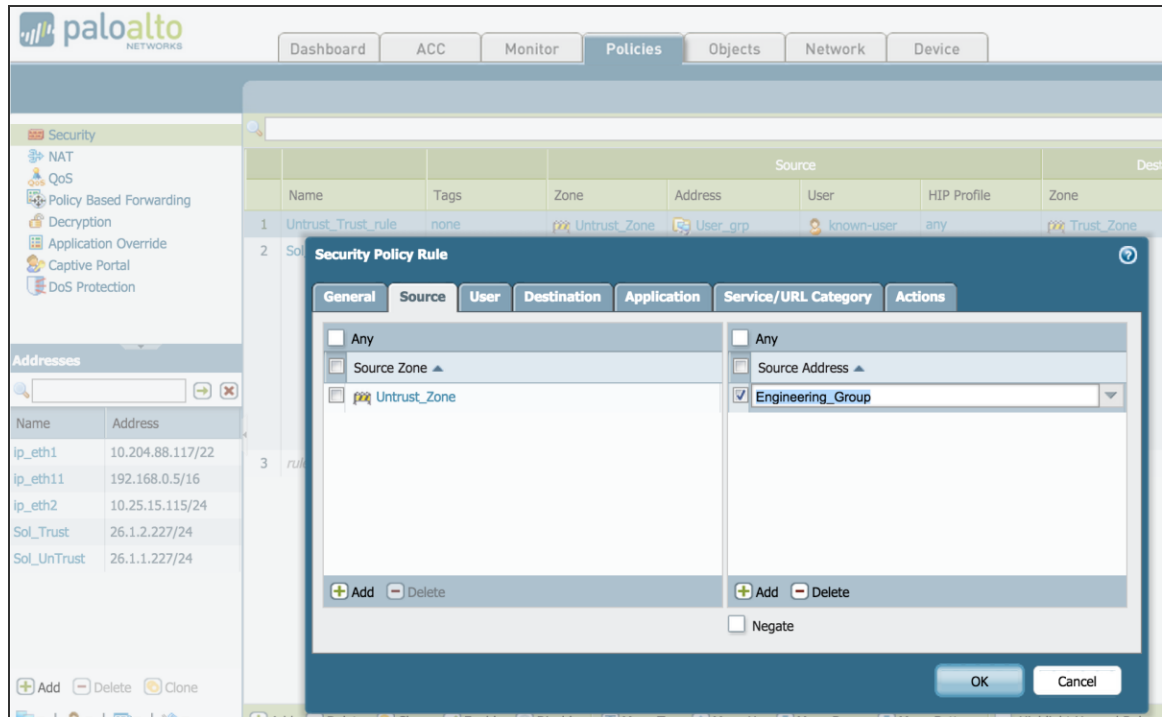
Dynamic discovery of users and their roles is not supported on the Palo Alto Networks firewall.

Configuring Security Policies

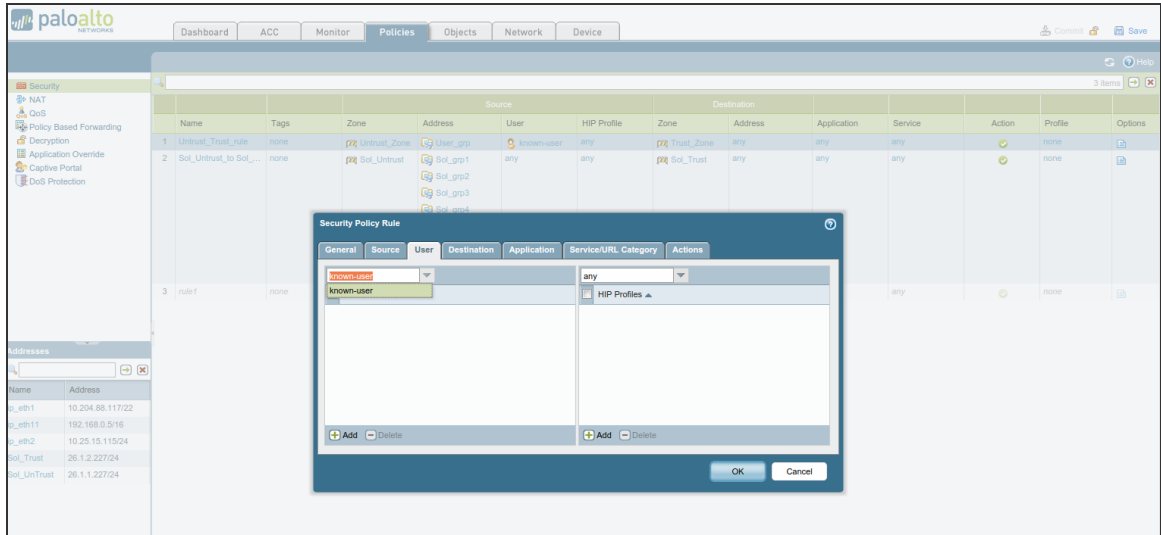
Security policies protect network assets from threats and disruptions and aid in optimally allocating network resources for enhancing productivity and efficiency in business processes. On the Palo Alto Networks firewall, security policies determine whether to block or allow a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service.

To configure security policies associated with dynamic address groups:

1. Select **Palo Alto Networks > Policies > Security**.
2. Click Add to create a new security policy rule. In the Source Address tab, select the previously-configured address group, as shown in figure.

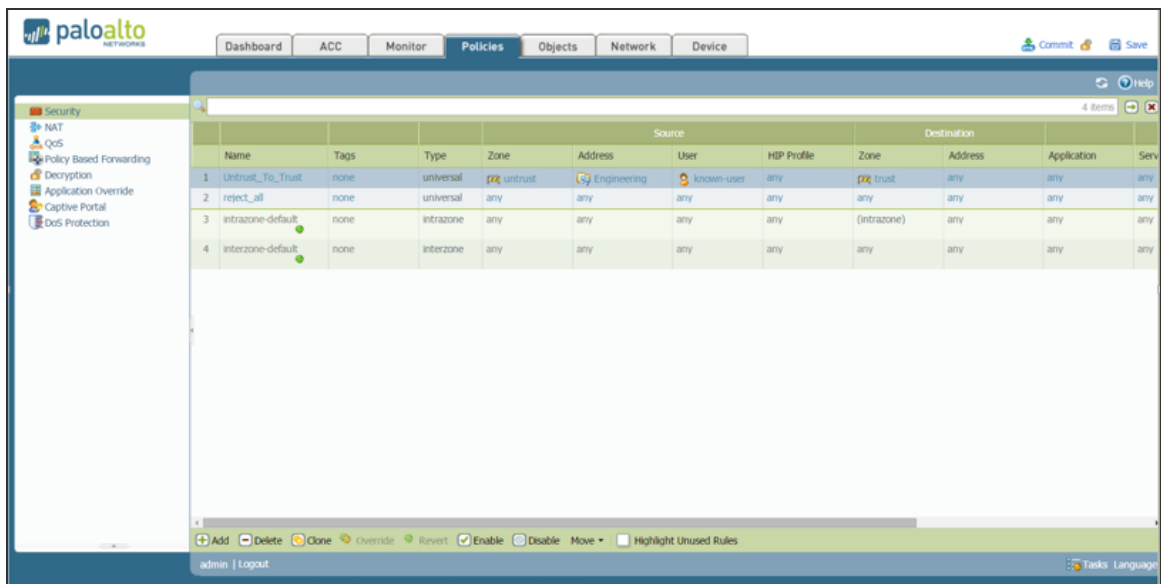


- In the User tab, enable **known-user**.



i When the **known-user** is enabled, the resource access is revoked immediately once the user disconnects from IPS.

- Configure the other options to meet your security requirements. Traffic from the endpoint is allowed or blocked based on the action chosen under the Action tab.
- Click **Commit** to complete the configuration. The completed security configuration on the Palo Alto Networks firewall is shown below.



Configuring PAN Device Certificates

PAN device certificate validation enhances the security between IPS and the PAN device. It allows IPS to verify whether the server certificate is from a trusted source. This topic describes how to configure the IPS for validating device certificates, creating certificates on PAN, and checking the validity of the certificate.

Creating a Certificate Signing Request (PAN 6.0 and later)

To create a Certificate Signing Request (CSR) for sending to public third-party Certificate Authority (like Verisign, Globalsign, Entrust, and so on). For more information, see <https://www.paloaltonetworks.com/documentation/60/pan-os/pan-os/certificate-management/obtain-certificates>

1. Select **Device > Certificate Management > Certificates > Device Certificates**.

Generate Certificate

Certificate Name: PANcertificate

Common Name: www.example.com
IP or FQDN to appear on the certificate

Signed By: External Authority (CSR) ▼

Certificate Authority

OCSP Responder: ▼

Cryptographic Settings

Algorithm: RSA ▼

Number of Bits: 2048 ▼

Digest: sha256 ▼

Expiration (days): 365

Certificate Attributes

Type	Value
<input checked="" type="checkbox"/> Country	DE
<input type="checkbox"/>	

2. Enter a **Certificate Name** (save this name for later).
3. In the Common Name field, enter the IP address of the interface where you will configure the service that will use this certificate.

4. Select the **Certificate Authority (CA)** check box for self-signed root CA certificate. Exporting the CSR and Importing the Signed Certificate are not applicable for self-signed certificates.



Uncheck the **Certificate Authority** check box if you are using enterprise CA, or trusted third-party CA certificates.

5. Complete the remaining details such as Country, Organization, and so on. Check with the Certificate Authority (CA) about their requirements for Certificate Attribute formatting and criteria.
6. Click **Generate**.



Ensure that the SSL/TLS service profile is enabled while creating the server certificate.

Exporting the CSR and Importing the Signed Request

Once the CSR is created, you must export the CSR to a third-party CA for signature.

To export the CSR:

1. Click the check box next to the Certificate Name.
2. Click **Export** and save the file.
3. Send the exported CSR to a third-party Certificate Authority. The CA will respond with a signed certificate.

Once the CA responds with the signed certificate, you must import the signed certificate from the certificate authority.

To import the signed certificate:

1. Note the name, including capitalization, of the certificate to import. (This must match the CSR request from above.)
2. Click **Import**.
3. In the Import Certificate dialog, type the name of the pending certificate. It must match exactly.
4. Go to the signed certificate received from the Certificate Authority and click OK.
5. Do not click the **Import Private Key** check box.

6. Depending on the certificate authority used, it may be necessary to chain the intermediate certificate with the server certificate and import it before completing this step.
7. Click **OK**.

Importing the Certificate on IPS

You can use the Trusted Server CAs page to import the trusted root certificate.

To configure device certificate verification:

1. Select **System > Trusted Server CAs > Import Trusted Server CA**.
2. Click **Browse** and select the certificate file.
3. Click **Import Certificate**. The Trusted Server CA page appears.
4. Verify if the certificate is imported successfully and click **Done**.
5. Click **Configuration > Certificates > Trusted Server CAs** and verify that the certificate is from a trusted source.

Adding PAN Device to IPS

For complete information on configuration, See [Configuring PAN Infranet Enforcer in IPS](#).



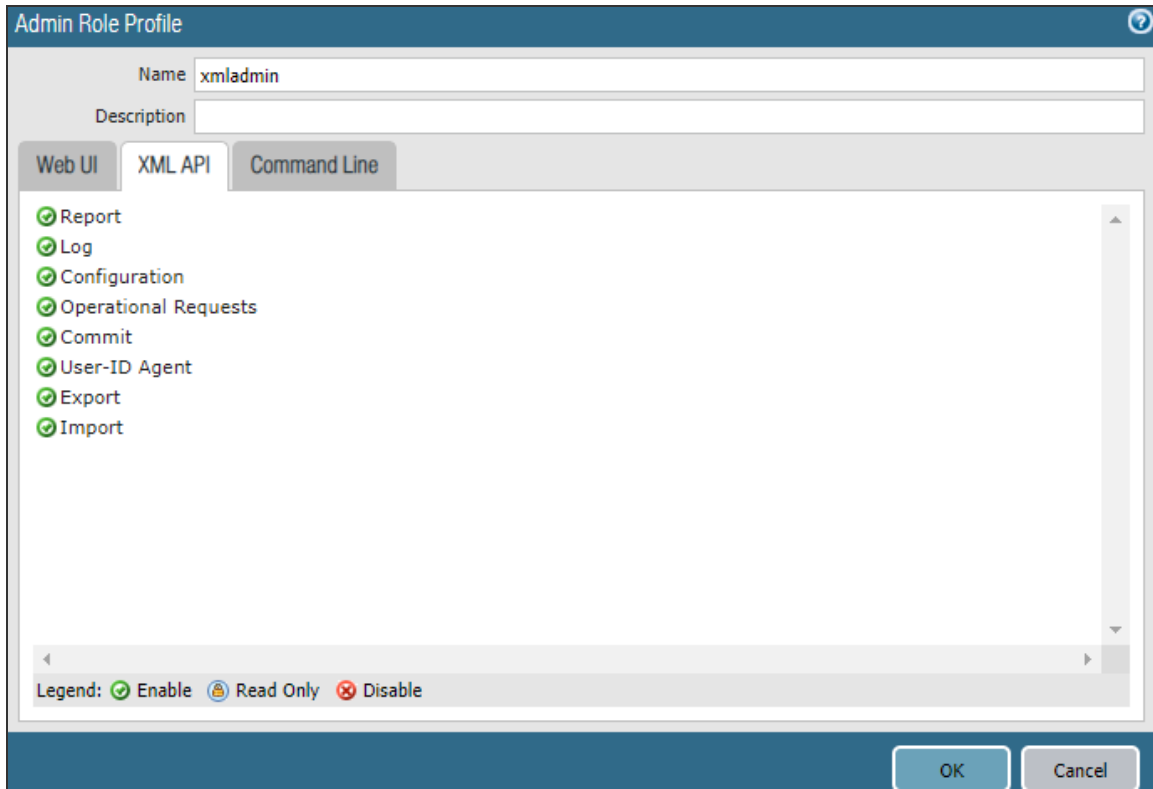
If the server certificate is not valid the user will see the following error message. Error: Failed to Retrieve API Key. Peer Certificate cannot be authenticated with known CA certificates.

Troubleshooting

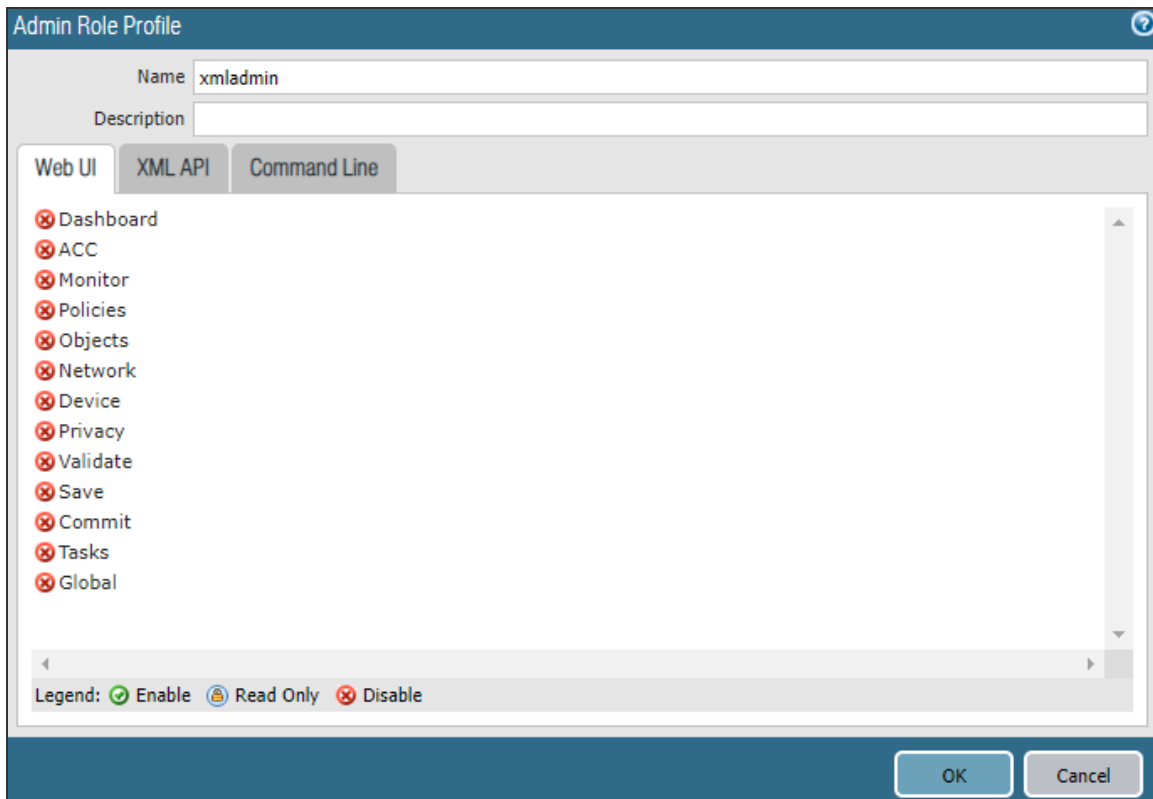
You can use the following CLI commands on the Palo Alto Networks firewall for troubleshooting:

- *show user ip-user-mapping all* - Displays the table of user identities mapped to IP addresses.
- *show object registered-address all* - Displays the table of addresses with user information associated.

For identity management using Palo Alto Networks firewall only minimum Admin role permissions are sufficient. Ensure that the XML API rights on the Palo Alto Networks UI is enabled as shown in the below screenshot.



Admin can choose to disable other options from the Web UI tab of the Palo Alto Networks UI as per the security requirement.



Unsupported Features

The following features are not supported:

- Captive portal
- IPsec Enforcement
- Dynamic Auth Table Allocation

For federated access across multiple policy servers / firewall enforcers federated single sign-on for Ivanti Connect Secure tunneled traffic, see [Provisioning ICS sessions to PAN/Check Point/FortiGate Firewall](#)

For information on Alert based Admission Control, see Admission Control using Palo Alto Networks Firewall

Enforcement using FortiGate Firewall

Overview

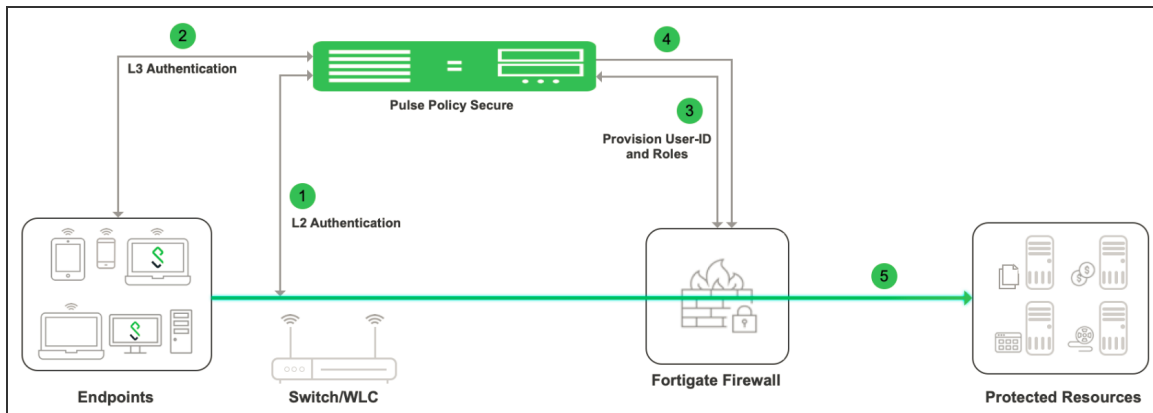
This chapter covers the FortiGate firewall integration with IPS using RADIUS accounting messages. FortiGate Firewall "SSO using RADIUS accounting records" feature allows FortiGate to receive user and group information details using RADIUS accounting messages.

FortiGate firewall can authenticate users transparently who have already authenticated on an external RADIUS server. The security policy applies the appropriate profiles based on the user group to which the user belongs. RADIUS SSO is relatively simple because the FortiGate unit does not interact with the RADIUS server, it only monitors RADIUS accounting records that the server forwards (originating from the RADIUS client, i.e Ivanti Policy Secure). These records include the user's IP address, user group and user name.

FortiGate needs to know the user's endpoint identifier (usually IP address) and RADIUS user group.

Deployment of IPS using FortiGate Firewall

This section describes the integration of IPS with FortiGate firewall.



The authentication process is described below:

1. The user is authenticated on IPS after validating the host check policy to ensure that the endpoints meets the corporate policy.
2. IPS learns the endpoint IP using RADIUS accounting(L2) or L3 connection.
3. The User Id, IP address and role(s) are provisioned to the firewall.

4. Ivanti Policy Secure shares the User Id, IP address and role information with FortiGate firewall in the form of a RADIUS accounting packet.
5. The FortiGate firewall maps the user to a specific security policy and then provides the required access.

If multiple firewall devices are configured, then the user's information will be provisioned to all the devices. The user's information will be sent to the firewall only if user's role requires session to be provisioned.

Configuring IPS with FortiGate Firewall

To configure FortiGate firewall:

1. Select **Endpoint Policy > Infranet Enforcer**.
2. Click New Infranet Enforcer and select FortiGate Firewall in the Platform drop down.

Infranet Enforcer > Connection > New Infranet Enforcer

New Infranet Enforcer

▼ Infranet Enforcer

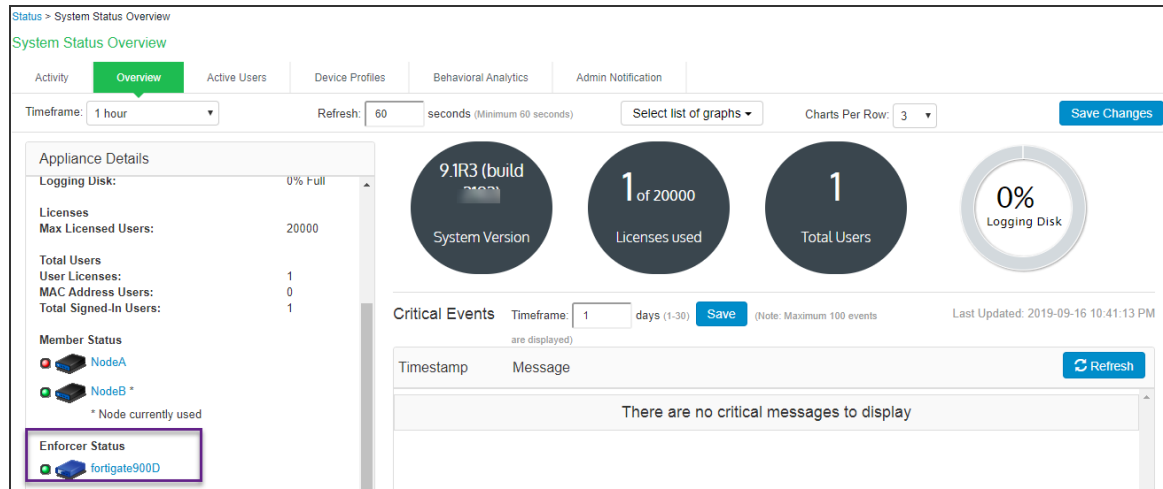
Platform:	FortiGate Firewall	Platform of this Infranet Enforcer.
* Name:	fortigate900D	Label to reference this Infranet Enforcer.
* IP Address:		IP Address of this Infranet Enforcer
* Shared Secret:	*****	Pre-Shared Secret
* Accounting Port:	1813	Port used for RADIUS accounting

[Save Changes](#)

* indicates required field

3. Enter the name of the Infranet Enforcer in the Name box.
4. Enter the IP address of FortiGate Firewall.
5. Enter the shared secret.
6. Enter the port number used for RADIUS accounting.
7. Click Save Changes. You must create security policies on the FortiGate firewall for traffic enforcement.

- Check the Status > Overview page for checking the status of the connection.



Configuring Auth Table Mapping Policy

To configure auth table mapping policies:

- Select **Endpoint Policy > Infranet Enforcer > Auth Table Mapping**.
- Click **New Policy**.
- Enter a name to label this auth table mapping policy.
- Select FortiGate as an enforcer in the Enforcer section, specify the Infranet Enforcer device(s) to which you want to apply this auth table mapping policy.
- In the Action section, specify auth table mapping rules for the specified Infranet Enforcer.
- Click **Save Changes**.

Configuring FortiGate Firewall

The FortiGate firewall detects traffic from an endpoint that matches a configured security policy using IPS RSSO record. It determines the role(s) associated with that user, and allows or denies the traffic based on the actions configured in the security policy.

To configure FortiGate firewall:

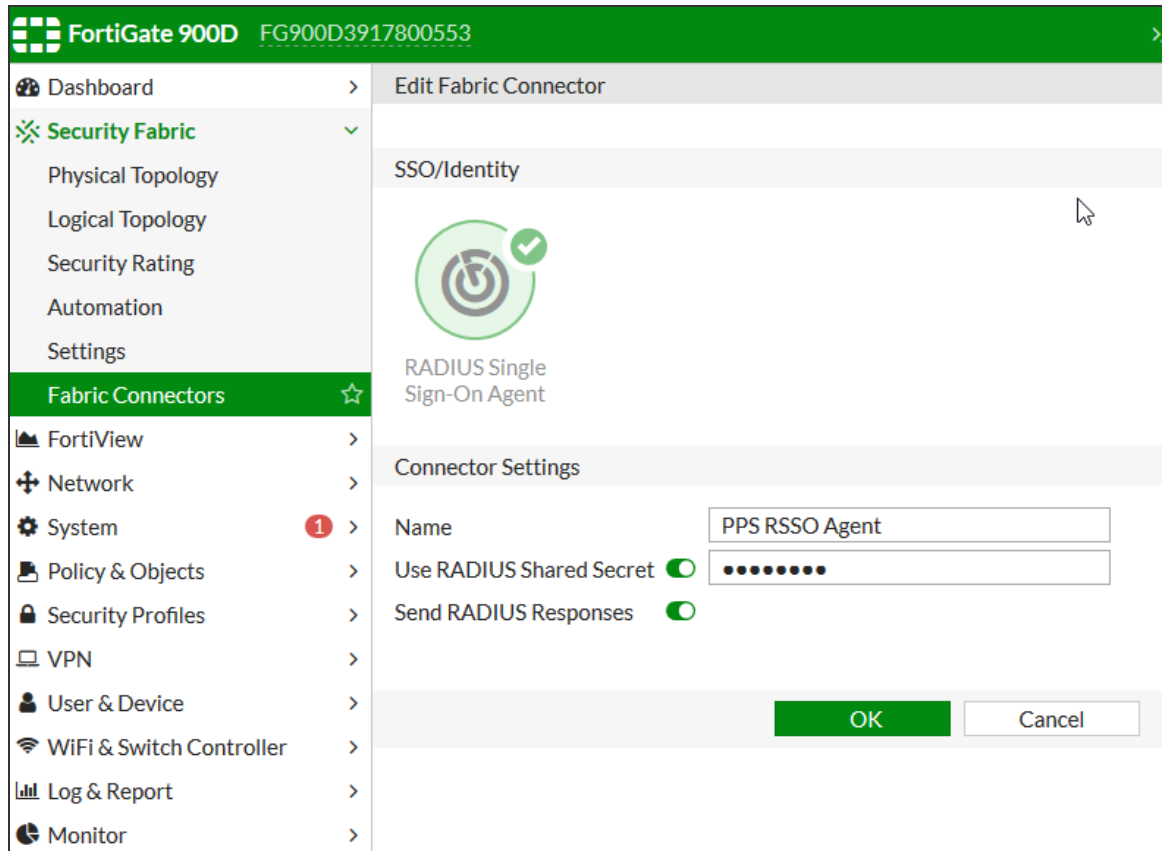
1. Select **System** > **Network** > **Interfaces**[datainterface] and enable **RADIUS Accounting** to allow the interfaces to listen for RADIUS Accounting Messages.

The screenshot shows the FortiGate 900D configuration interface for editing an interface. The left sidebar shows the navigation menu with 'System' selected, indicated by a red '1' and a right-pointing arrow. The main content area is titled 'Edit Interface' and displays the following configuration details:

- Interface Name: port10 (70:4C:A5:53:69:6C)
- Alias: [Empty text box]
- Link Status: Up (with a green up arrow icon)
- Type: Physical Interface
- Tags: Role is set to LAN (with an information icon and a dropdown arrow). There is an 'Add Tag Category' button below.
- Address: Addressing mode is set to Manual (highlighted in green). Other options are DHCP and Dedicated to FortiSwitch. IP/Network Mask is 10.255.0.4/255.255.255.0.
- Administrative Access: A grid of checkboxes for various protocols. Under the IPv4 section, 'RADIUS Accounting' is checked and highlighted with a purple box. Other checked protocols include HTTPS, HTTP, CAPWAP, SSH, PING, SNMP, and FortiTelemetry. Under the IPv6 section, FMG-Access and FTM are checked.

2. Select **Fabric Connector > Create New**, under **SSO/Identity** select **RADIUS Single Sign-On Agent**.

- Name: Enter a name for the entry
- Enter the RADIUS shared secret, which matches with IPS.
- Click **OK**.

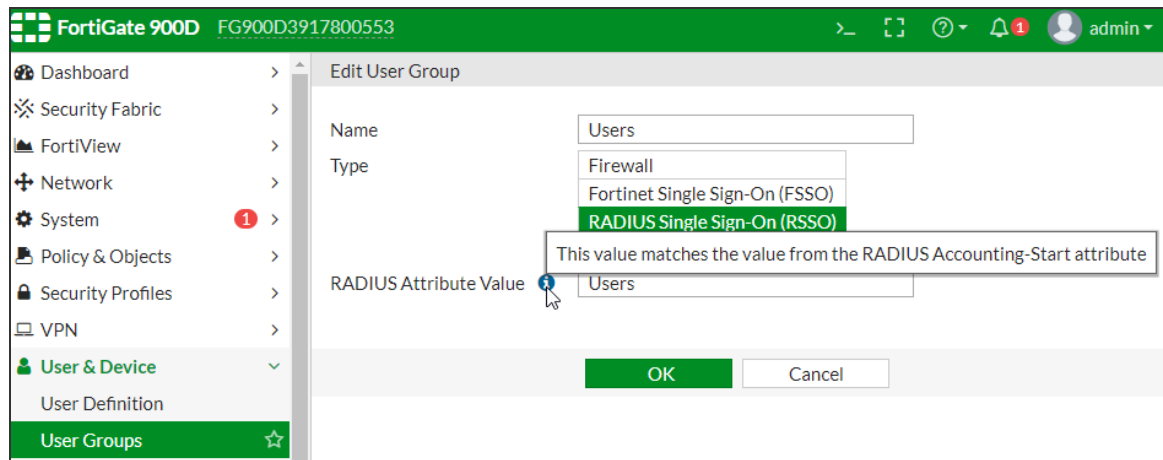


The screenshot displays the FortiGate 900D web interface. The top header shows the device name 'FortiGate 900D' and the ID 'FG900D3917800553'. The left sidebar contains a navigation menu with 'Fabric Connectors' highlighted. The main content area is titled 'Edit Fabric Connector' and shows the 'SSO/Identity' section. A green checkmark icon is visible next to the 'RADIUS Single Sign-On Agent' entry. Below this, the 'Connector Settings' section is visible, containing the following fields and controls:

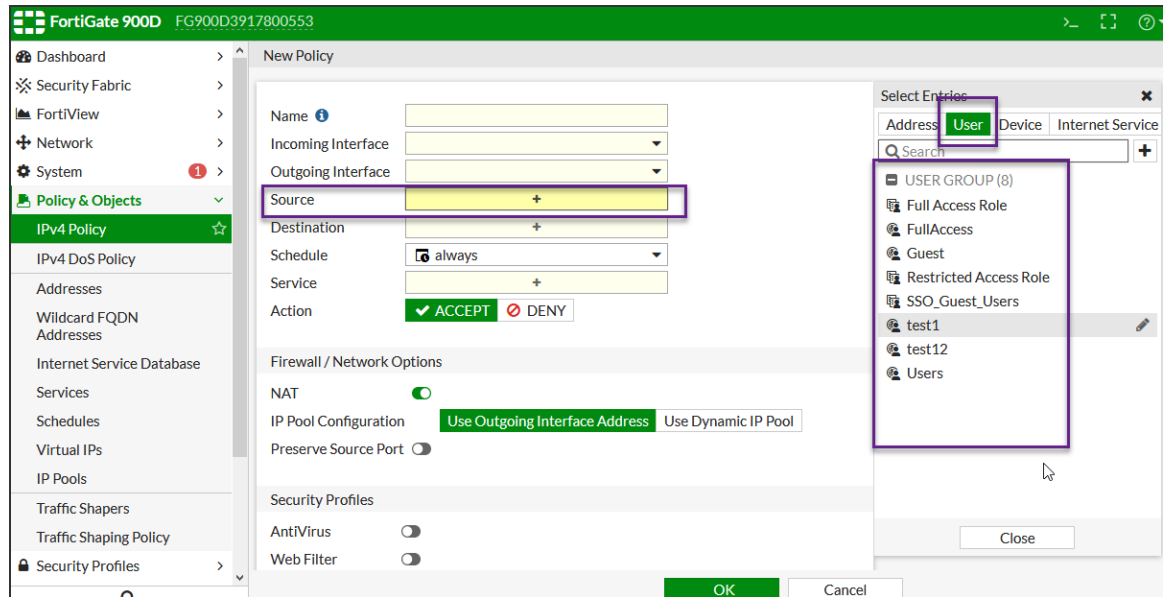
- Name:** A text input field containing 'PPS RSSO Agent'.
- Use RADIUS Shared Secret:** A toggle switch that is turned on, followed by a password input field containing ten dots.
- Send RADIUS Responses:** A toggle switch that is turned on.

At the bottom of the settings section, there are two buttons: a green 'OK' button and a white 'Cancel' button.

3. Create matching User groups. Select **User & Device > User Groups**. Click create New and enter the following data:
 - Name- Enter the name of the group. This name will appear in the firewall policy.
 - Type- Select RADIUS Single Sign-On as type.
 - RADIUS Attribute Value- Enter the User Role created on IPS to match the User Group in FortiGate.
 - Click **OK**.



4. Create a firewall policy to use the IPS enforcement groups just created. Select **Policy & Objects** > **IPv4 Policy**. Click Create New and create the policy based on the resource access restrictions to be enforced.



5. Disable overriding of the roles on FortiGate firewall when the same user logs in with a different device. The default behavior is to override the role information with the latest role received from IPS.

For example, if a same user login's to IPS from different devices (mobile/laptop) with different roles (Employee/Guest). Fortigate firewall overrides the role information with the latest role by default. To disable overriding with the latest roles "set sso-attribute-value-override disable".

```
config user radius
edit <My_Rsso>
set rspo enable
set sso-attribute-value-override enable/disable // Enable/Disable override old attribute
value with new value for the same endpoint.
end
```

Reports and Logging

1. You can monitor the RSSO Sessions on FortiGate firewall from CLI or GUI:

Using the FortiGate CLI, type:

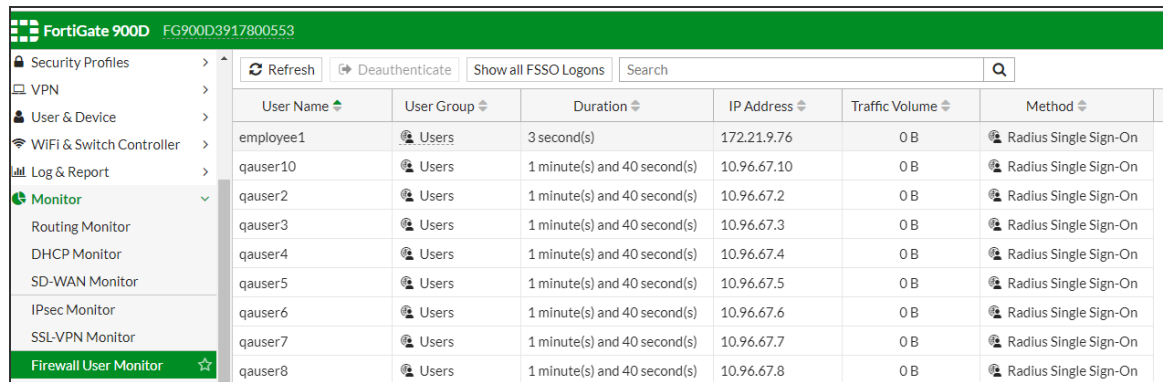
```
diag rso query ip <Ip-Address>
```

```
diag rso query rso-key
```

*Queries the RSSO database.

```
FG900D3917800553 # diag rso query ip 10.96.67.10
Querying IP '10.96.67.10'
Endpoint: qauser10
RSSO Key: Users
IP Addresses:
      IP: 10.96.67.10, Time left (hh:mm:ss): 07:59:56 **
```

2. Select **Monitor > Firewall user Monitor**. The list shows all the identity records.



The screenshot shows the FortiGate GUI interface for the Firewall User Monitor. The left sidebar contains navigation options: Security Profiles, VPN, User & Device, WiFi & Switch Controller, Log & Report, Monitor (selected), Routing Monitor, DHCP Monitor, SD-WAN Monitor, IPsec Monitor, and SSL-VPN Monitor. The main content area displays a table of user sessions with columns for User Name, User Group, Duration, IP Address, Traffic Volume, and Method. The table lists eight users (employee1 through qauser8) all belonging to the 'Users' group, with durations ranging from 3 seconds to 1 minute and 40 seconds, and all having 0 B of traffic volume. The method for all sessions is 'Radius Single Sign-On'.

User Name	User Group	Duration	IP Address	Traffic Volume	Method
employee1	Users	3 second(s)	172.21.9.76	0 B	Radius Single Sign-On
qauser10	Users	1 minute(s) and 40 second(s)	10.96.67.10	0 B	Radius Single Sign-On
qauser2	Users	1 minute(s) and 40 second(s)	10.96.67.2	0 B	Radius Single Sign-On
qauser3	Users	1 minute(s) and 40 second(s)	10.96.67.3	0 B	Radius Single Sign-On
qauser4	Users	1 minute(s) and 40 second(s)	10.96.67.4	0 B	Radius Single Sign-On
qauser5	Users	1 minute(s) and 40 second(s)	10.96.67.5	0 B	Radius Single Sign-On
qauser6	Users	1 minute(s) and 40 second(s)	10.96.67.6	0 B	Radius Single Sign-On
qauser7	Users	1 minute(s) and 40 second(s)	10.96.67.7	0 B	Radius Single Sign-On
qauser8	Users	1 minute(s) and 40 second(s)	10.96.67.8	0 B	Radius Single Sign-On

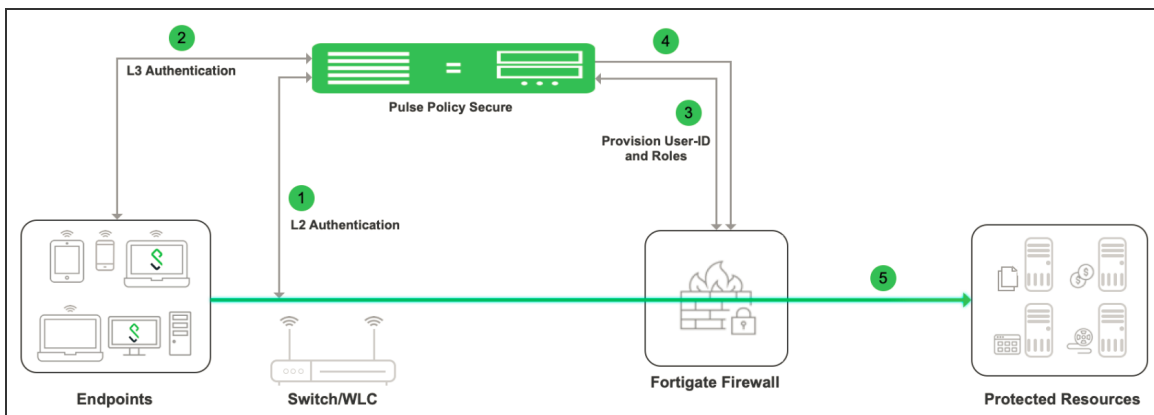
Identity Based Enforcement using FortiGate Products

Overview

IPS integration with the FortiGate firewall provides enhanced identity enabled enforcement with backend authentication and comprehensive compliance checks. This section describes the procedure to integrate IPS with FortiGate firewall using FortiAuthenticator, which acts as a syslog server. The FortiAuthenticator receives the syslog messages from IPS and then creates Fortinet Single Sign-on (FSSO) record which is then shared with FortiGate firewall. The firewall uses the FSSO information to either allow or block traffic based on the configured policy.

Deployment of IPS using FortiAuthenticator and FortiGate Firewall

This section describes the integration of IPS with FortiAuthenticator and FortiGate firewall. The IPS and Fortinet solution provides functionality for enforcing security policies on a per user and role basis.



The authentication process is described below:

1. The user is authenticated on IPS after validating the host check policy to ensure that the endpoints meets the corporate policy.
2. The syslog sessions are exported to FortiAuthenticator.

3. Identity information is parsed from the syslog message and is used to create an IP address to username mapping file within FortiAuthenticator. This information is shared with FortiGate firewall in the form of a FSSO record.
4. The FortiGate firewall maps the user to a specific resource access policy and then provides the required access.

Configuring IPS with FortiAuthenticator

The IPS configuration requires defining the FortiAuthenticator as the syslog server on IPS. The Syslog sever uses the filter created in the User Access Log Filters for receiving and parsing the logs.

Creating Custom Filter for User Access Logs

To create a custom filter in IPS:

1. Select **System > Log/Monitoring > User Access > Filters**.
2. Click **New Filter**.
3. Enter the filter name.
4. Under Export Format, select **WELF**.
5. Click **Save** to save the filter.

The screenshot shows the 'New Log filter' configuration page in the FortiGate web interface. The breadcrumb path is 'Log/Monitoring > User Access > Filters > New Log filter'. The page title is 'New Log filter'. There are tabs for 'Events', 'User Access', 'Admin Access', 'Sensors', 'Client Logs', 'SNMP', 'Statistics', and 'Advanced Settings'. The 'User Access' tab is active. Below the tabs, there are sub-tabs for 'Log', 'Settings', and 'Filters'. The 'Filters' sub-tab is active. The 'Filter' section has a 'Filter Name' field containing 'FSSO' and a checkbox for 'Make default for syslog and archiving filter selection'. Below this is a 'Query' section and an 'Export Format' section. The 'Export Format' section has radio buttons for 'Standard', 'WELF', 'W3C', and 'Custom'. The 'WELF' radio button is selected. Below the radio buttons is a 'Format' field with a text area containing the following WELF log format string:


```
id=firewall time=%date% %time% pri=%syslogcode%
fw=%localip% vpn=%node% user=%user% realm=%realm%
roles=%role% proto=%protocol% src=%sourceip%
dst=%remoteip% dstname=%remotehost% type=vpn
```

 At the bottom of the page are 'Save' and 'Cancel' buttons.

Editing the Custom Filter

To edit the custom created filter:

1. From the **Log Filters** screen, click the filter name and edit the filter.
2. Under **Export Format**, select **Custom** format.
3. Edit the **ID** with the filter name. For example, id=FSSO.
4. Click **Save**.

The screenshot shows the 'New Log filter' configuration page in the FortiGate web interface. The breadcrumb trail is 'Log/Monitoring > User Access > Filters > New Log filter'. The page title is 'New Log filter'. There are tabs for 'Events', 'User Access', 'Admin Access', 'Sensors', 'Client Logs', 'SNMP', 'Statistics', and 'Advanced Settings'. The 'User Access' tab is active. Below the tabs, there are sub-tabs for 'Log', 'Settings', and 'Filters'. The 'Filters' sub-tab is active. The 'Filter' section has a 'Filter Name' field containing 'FSSO' and a checkbox for 'Make default for syslog and archiving filter selection'. Below this is a 'Query' section and an 'Export Format' section. The 'Export Format' section has radio buttons for 'Standard', 'WELF', 'W3C', and 'Custom'. The 'Custom' radio button is selected. A dropdown menu is open, showing a custom format string: 'id=FSSO time=%date% %time% pri=%syslogcode% fw=%localip% vpn=%node% user=%user% realm=%realm% roles=%role% proto=%protocol% src=%sourceip% dst=%remoteip% dstname=%remotehost% type=vpn'. At the bottom of the page are 'Save' and 'Cancel' buttons.

Configuring Syslog Server

You can configure IPS to send logs to FortiAuthenticator syslog server.

To configure the syslog server:

1. Select **System > Log/Monitoring > User Access > Settings Policy** and click **New Policy**.
2. Under **Select Events to Log**, retain the default settings.
3. Under **Syslog Servers**, create a new Syslog server with the following details:
 - Server name/IP- Enter the fully qualified domain name or the IP address for the syslog server (FortiAuthenticator).
 - Facility- Select **LOCAL0** as the facility level.
 - Type- Select **UDP** as the connection type.
 - Filter- Select the custom created filter format.
4. Click **Add** and then click **Save Changes**.



You must add FortiAuthenticator as a syslog server in all the nodes in a clustering environment.

The screenshot shows the FortiGate web interface for configuring log settings. The breadcrumb path is 'Log/Monitoring > Events > Log settings'. The 'Log settings' page has tabs for 'Events', 'User Access', 'Admin Access', 'Sensors', 'Client Logs', 'SNMP', 'Statistics', and 'Advanced Settings'. The 'Events' tab is active, and the 'Settings' sub-tab is selected. There are 'Save Changes' and 'Reset' buttons at the top. Below are expandable sections for 'Maximum Log Size', 'Select Events to Log', and 'Syslog Servers'. A note states: 'Events are logged locally. You can also log them to one or more external Syslog servers.' A 'Delete' button is present above a table. The table has columns for 'Server name/IP', 'Facility', 'Type', 'Client Certificate', and 'Filter'. One entry is shown with '10.96.71.4' in the IP field, 'LOCAL0' in the Facility dropdown, 'UDP' in the Type dropdown, 'Select Client Cert' in the Client Certificate dropdown, and 'FSSO: Custom' in the Filter dropdown. An 'Add' button is to the right of the first row. 'Save Changes' and 'Reset' buttons are at the bottom.

Server name/IP	Facility	Type	Client Certificate	Filter
10.96.71.4	LOCAL0	UDP	Select Client Cert	FSSO: Custom

Configuring FortiAuthenticator

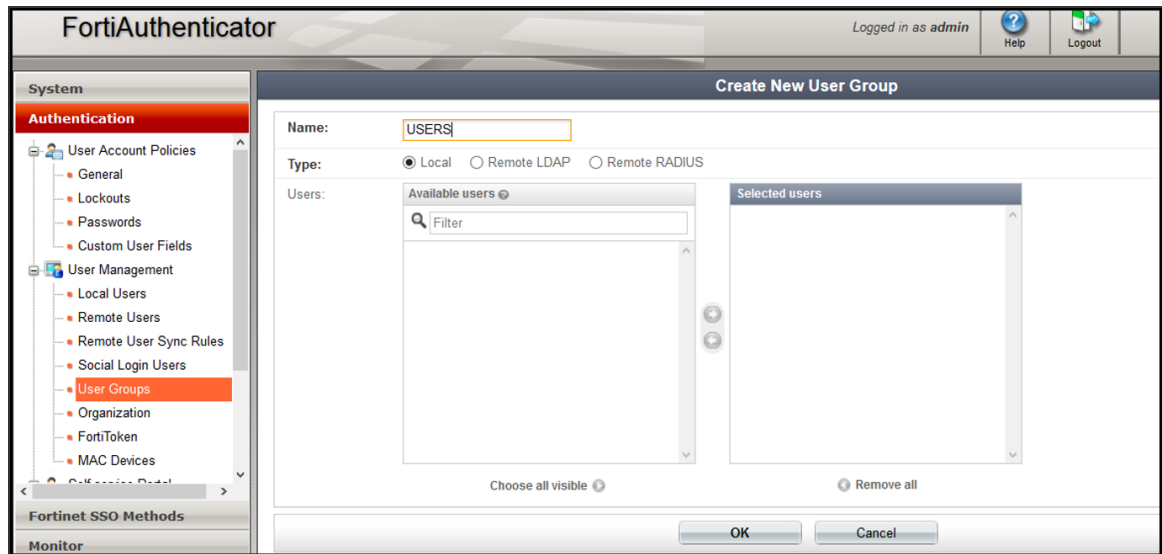
You must add IPS as a syslog source in FortiAuthenticator to parse the information.

Prerequisite:

- Ensure that the FortiAuthenticator instance is communicating on the network and is reachable from the IPS appliance's management interface.
- Select **System > Network > Interfaces**, select the port and enable the FortiGate FSSO, FortiClient FSSO and Syslog services on FortiAuthenticator interface, which communicates with IPS and FortiGate firewall.

To configure FortiAuthenticator:

1. Create a Local user group with the names which matches the name IPS will send as the 'Group=' value in your Syslog messages. Select **Authentication > User Management > User Groups** and click Create New. Create the groups with the following data:
 - Name- Enter the same names, which is received from IPS, For example, Users.
 - Type- Select Local as type.
 - Click **OK**.



2. Create a syslog matching rule. Select **Fortinet SSO methods > SSO > Syslog Sources**. In the upper right corner, from the 'View' drop down choose matching rules and click **Create New** and give the following data:

- **Name:** Enter the name for the syslog Rule.
- **Trigger:** Enter the filter name created in IPS. For example, id=FSSO
- **Auth Type Indicators:** Enter strings to differentiate between the types of user activities. For example, **Logon:** AUT24803
- **Update:** AUT23524
- **Logoff:** AUT22673
- **Username field:** Define the semantics of the username field, where {{user}} indicates where the username is extracted from. For example: user= {{: username}}
- **Client IP field:** Define the semantics of the client IP address. For example, src={{:client_ip}}
- **Group field:** Define the semantics of the group. For example: roles=" {{: group}}"



There is a trailing space after the User, IP, and Group fields. The parser treats the trailing space as an ending character after the variable portion of the field. The parsing fails if the trailing space is omitted.

- **Group List Separator:** SSO syslog feed can parse multiple groups if the names are separated by a plus (+) symbol or a comma (,). Use the Group list separator to specify the separator.
- **Test Rule:** Enter a sample log message into the text box, then select Test to test that the desired fields are correctly extracted.

- Click **OK** to add the new matching rule.

The screenshot shows the FortiAuthenticator web interface. The top navigation bar includes 'System', 'Authentication', 'Monitor', 'Certificate Management', and 'Logging'. The 'Authentication' section is expanded to show 'Fortinet SSO Methods', with 'Syslog Sources' selected. The main configuration area is titled 'Edit Syslog Matching Rule' and contains the following fields:

- Name:** Rule configuration
- Description:** Rule configuration to extract parameters from incoming syslog message
- Fields to Extract:**
 - Trigger:** id=FSSO
 - Auth Type Indicators:**
 - Logon:** AUT24414
 - Update:** AUT23524
 - Logoff:** AUT22673
 - Username field:** user={{username}}
 - Client IPv4 field:** src={{client_ip}}
 - Client IPv6 field:** e.g., Framed-IPv6-Address={{client_ipv6}};
 - Group field:** roles={{group}}*
 - Group list separator:** ,
- Test Rule:**
 - Test the matching rule above by entering a sample log line to parse below.
 - Enter a sample log line
 - Test button



For the Logon and Logoff indicators, the data specified will vary depending on the installation and depending on your syslog message contents. In this example, when a user logs in the message ID created is AUT24414 and is considered as a Logon event on FortiAuthenticator. When the role change happens as part of periodic host check updates, the message ID created by IPS is AUT23524. A sign-out event is considered a 'Logoff' event on FortiAuthenticator, and the identity is removed from the user group, thus, failing to match policy.

4. Create a Syslog source, Select Fortinet SSO methods > SSO > Syslog Sources. In the upper right corner, from the 'View' drop down choose Syslog Source and click Create New and provide the following data:
 - Name- Enter a name for the source
 - IP address- Enter the IP address of IPS server
 - Matching rule- Select the requisite matching rule created above.
 - SSO user type- Select External as the user type.

The screenshot shows the FortiAuthenticator web interface. The left sidebar contains a navigation tree with 'Fortinet SSO Methods' expanded to 'Syslog Sources'. The main content area is titled 'Create New Syslog Source' and contains the following fields:

- Name: Pulsesecure
- IP address: x.x.x.x
- Matching rule: Pulse
- SSO user type: External, Local users, Remote users

Buttons for 'OK' and 'Cancel' are visible at the bottom right of the form.



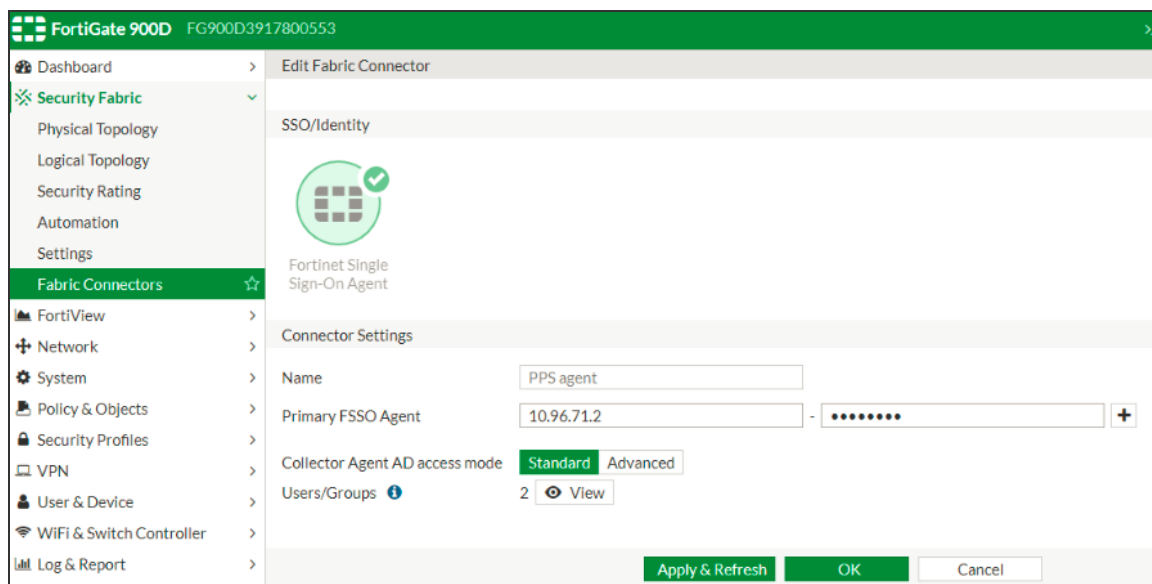
You must add all the cluster node IP's (not cluster VIP's) in the FortiAuthenticator when using a IPS cluster setup.

Configuring FortiGate Firewall

The FortiGate firewall detects traffic from an endpoint that matches a configured security policy using the FortiAuthenticator FSSO record. It determines the role(s) associated with that user, and allows or denies the traffic based on the actions configured in the security policy.

To configure FortiGate firewall:

1. (Applies to Release 6.0.*) Create the FortiAuthenticator as an FSSO agent in the FortiGate Firewall. Select **Fabric Connector > Create New**, under SSO/Identity select **Fortinet Single Sign-On Agent**.
 - Name: Enter a name for the entry
 - Primary FSSO Agent: Enter the IP address of the FortiAuthenticator appliance, and the password* used to communicate with it.
 - Click **Apply & Refresh** to test your configuration. If correct, the users /groups area will automatically populate

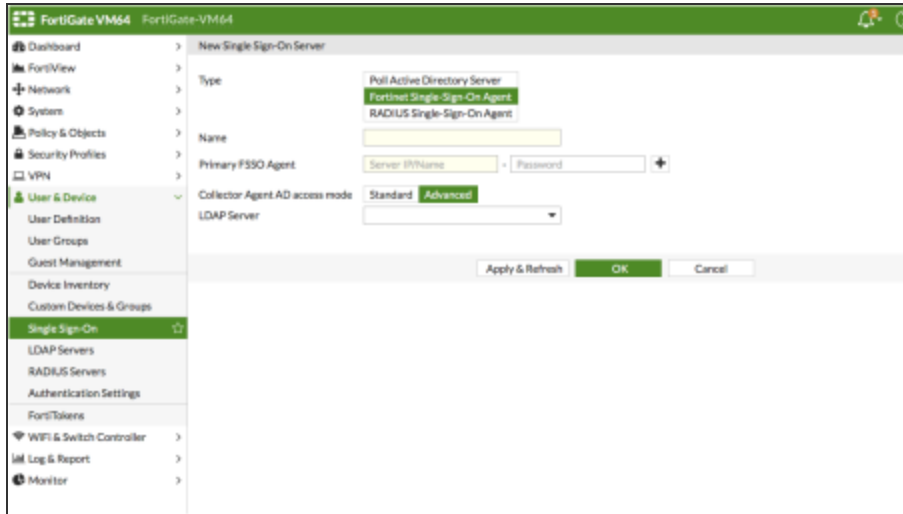


(Applies to Release 5.6.*) Create the FortiAuthenticator as an FSSO agent in the FortiGate Firewall. Select **User & Device > Single Sign-On** and click **Create New** and enter the following data.

- Type: Fortinet Single-Sign-On Agent
- Name: Enter a name for the entry
- Primary Agent IP/Name: Enter the IP address of the FortiAuthenticator appliance, and the password* used to communicate with it.

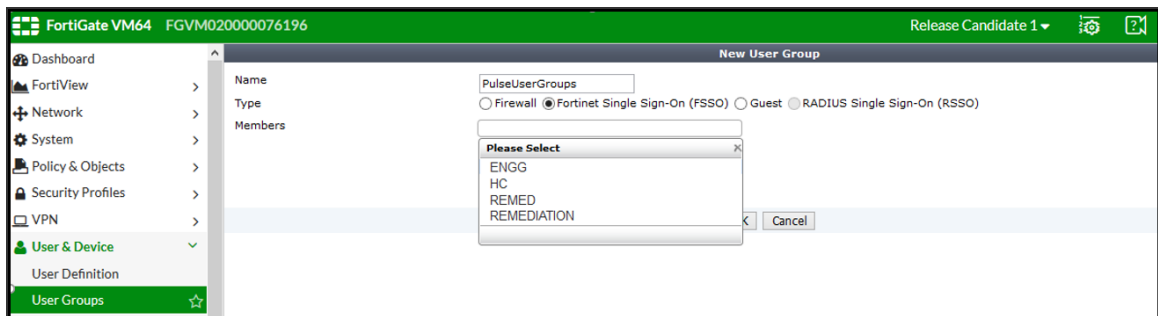
*This is the same as the secret key configured on FortiAuthenticator in the Fortinet SSO Methods > General section.

- Click **Apply & Refresh** to test your configuration. If correct, the users /groups area will automatically populate.

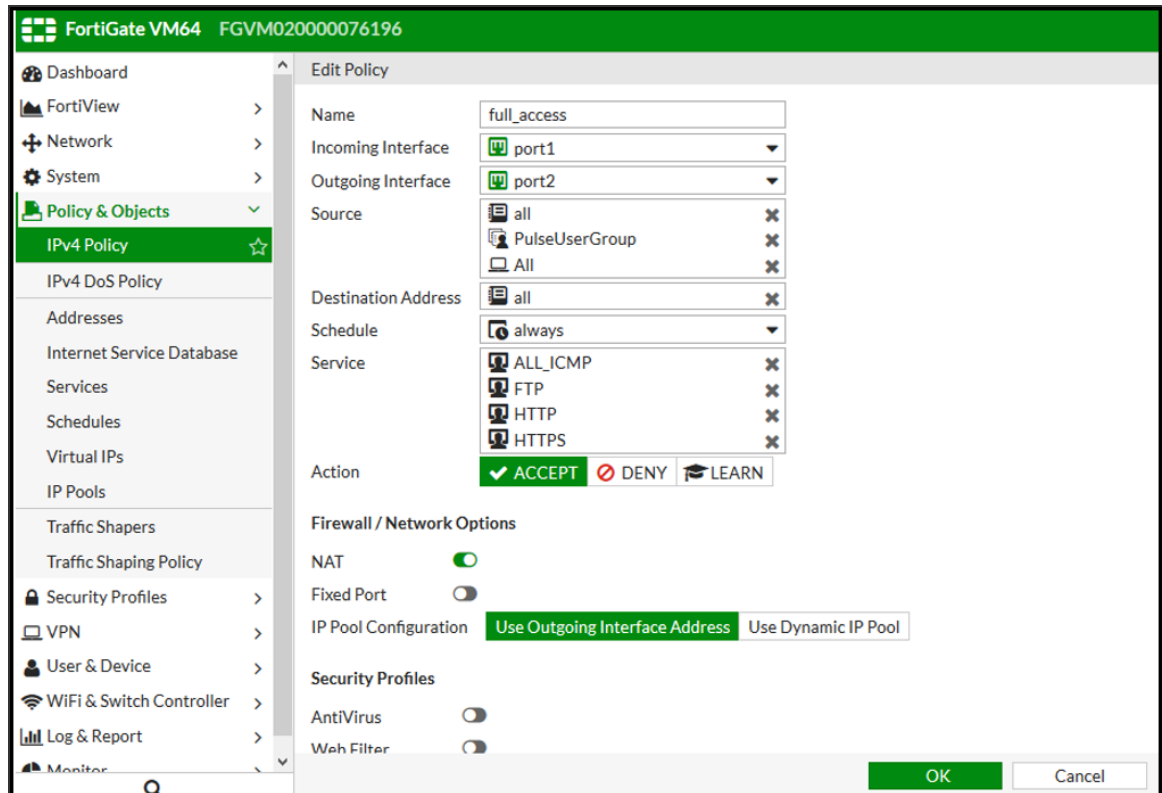


2. Create matching User groups. Select **User & Device > User Groups**. Click create New and enter the following data:

- Name- Enter the name of the group. This name will appear in the firewall policy.
- Type- Select **Fortinet Single Sign-On** as type.
- Select the matching User group created on FortiAuthenticator and Click **OK**.



3. Create a firewall policy to use the IPS enforcement groups just created. Select **Policy & Objects** > **IPv4 Policy**. Click Create **New** and create the policy based on the resource access restrictions to be enforced.

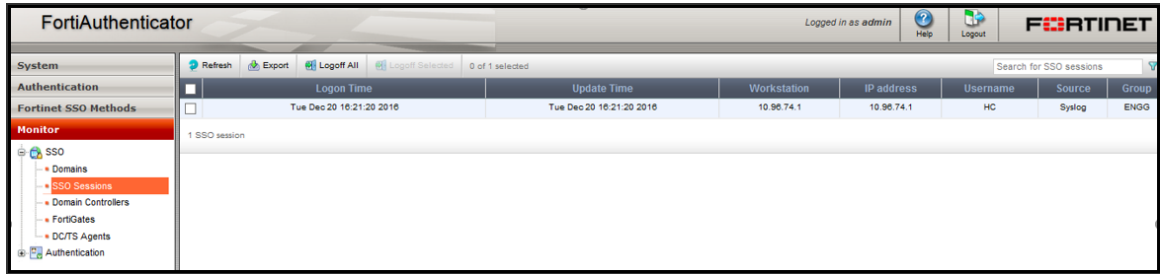


Reports and Logging

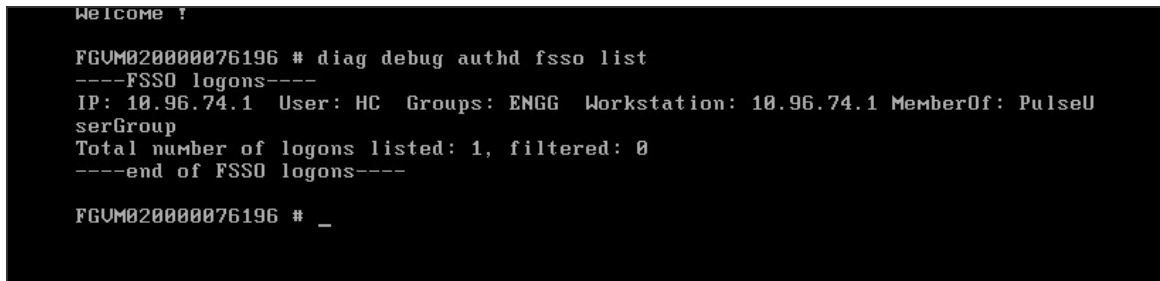
You can verify if the syslog messages are reaching the FortiAuthenticator by doing a packet capture on the FortiAuthenticator Interface.

1. Select **System** > **Network** > **Packet Capture** and select the interface which is used to communicate with the IPS and click **Start capture** button. Once packet capture is done stop the capture and download the packets and view it using any tool like wireshark.

- To view identity records from the FortiAuthenticator GUI, Select **Monitor > Sessions**. The list shows the records parsed through syslog.



- You can monitor the FSSO Sessions on FortiGate firewall from CLI or GUI:
Using the FortiGate CLI, type: `diag debug authd fssso list`
The command displays identity records received from FortiAuthenticator.



- Select **Monitor > Firewall user Monitor**. The list shows all the identity records.



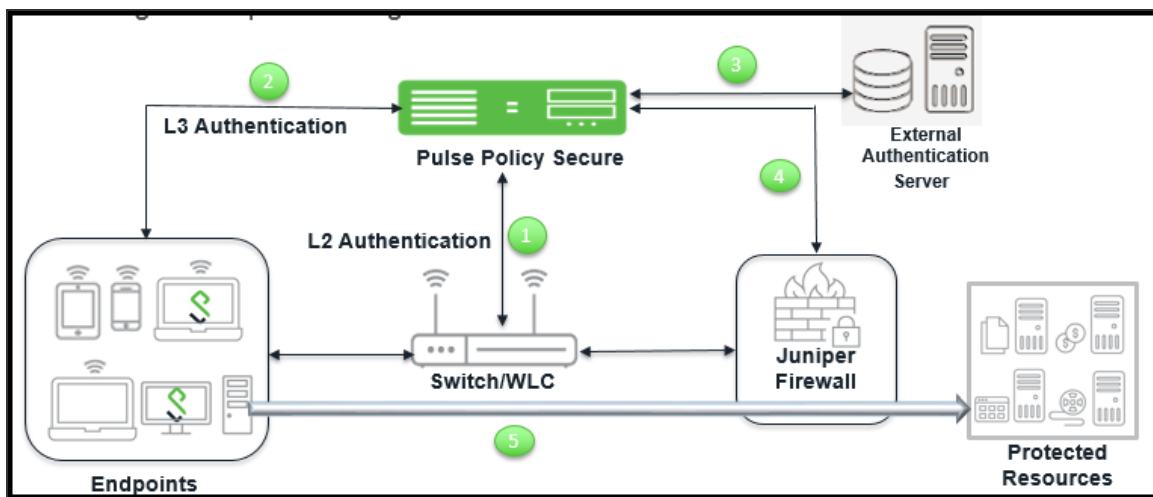
Enforcement using SRX Series Firewall

Overview

IPS delivers a layer 3 network access control solution when deployed with Juniper SRX firewall. The IPS is the Layer 2 or Layer 3 policy decision point that determines which users and endpoints can access protected resources. You can use Juniper Networks SRX firewall to serve as the enforcement point to provide the protection to ensure that network assets are secured. IPS authenticates users, ensures that endpoints meet security policies, and serves resource access policy information to Juniper Networks SRX devices.

Deployment of IPS using SRX Firewall

This section describes the integration of IPS with SRX firewall. The IPS and SRX firewall solution provides functionality for enforcing application level security policies on a per user and role basis. It also delivers granular level access control so that it can be easily managed through IPS.



The authentication process is described below:

1. The endpoint connects to switch to perform the layer 2 authentication with IPS.
2. IPS communicates with authentication server and performs the layer 3 authentication along with host check to ensure that the endpoints meet the corporate policy.

3. The external authentication server such as AD/LDAP confirms the role and sends the entries to IPS.
4. IPS provisions the auth table on SRX firewall with changes in role information if any.
5. The SRX series firewall maps the user to a specific resource access policy and then provides the required access.

Configuring IPS with SRX Firewall

The IPS connects with the SRX device over an SSL connection. To enable the connection between the two devices, you must specify the password and serial number of the SRX firewall. The SRX firewall initiates the connection to IPS. IPS presents its SSL server certificate to the SRX device. Optionally, you can configure the SRX device to verify the certificate and to specify constraints with which IPS must comply.

The SRX device and IPS perform mutual authentication with the proprietary JUEP-MAUTH challenge-response authentication based on the password configured. For security reasons, the password is not included in the message sent to IPS. After the SSL handshake, all further communication between the IPS device and the SRX device occurs over the SSL connection. The SRX device acts as a client and the IPS device as server.

Configuring SRX Infranet Enforcer in IPS

To configure a SRX Firewall Infranet Enforcer in IPS:

1. Select **Endpoint Policy > Infranet Enforcer**.

The screenshot shows the 'Infranet Enforcer Connection' configuration page. The page has a breadcrumb 'Infranet Enforcer > Infranet Enforcer Connection' and a title 'Infranet Enforcer Connection'. There are four tabs: 'Connection' (active), 'Resource', 'IPsec', and 'Auth Table Mapping'. Below the tabs, there is a description: 'A connection policy specifies the connection between the Pulse Policy Secure and Infranet Enforcer.' There are three buttons: 'New Enforcer...', 'Duplicate...', and 'Delete...'. Below the buttons, there is a dropdown menu set to '10' records per page and a search box. At the bottom, there is a table with the following columns: 'Enforcer', 'Serial Numbers', 'Location Group', 'Platform', 'Version', 'FIPS', and 'IP Address'. The table is currently empty.

Enforcer	Serial Numbers	Location Group	Platform	Version	FIPS	IP Address

- Click **New Infranet Enforcer** and select **Junos SRX Firewall** in the Platform drop down.

The screenshot shows the 'New Infranet Enforcer' configuration page. The breadcrumb trail is 'Infranet Enforcer > Connection > New Infranet Enforcer'. The page title is 'New Infranet Enforcer'. Under the 'Infranet Enforcer' section, there are the following fields:

- Platform:** A dropdown menu with 'JUNOS SRX' selected. The tooltip says 'Platform of this Infranet Enforcer.'
- * Name:** A text input field. The tooltip says 'Label to reference this Infranet Enforcer.'
- * Password:** A text input field. The tooltip says 'Connection password.'
- * Serial number(s):** A text area. The tooltip says 'One per line.'
- Location Group:** A dropdown menu with '- No 802.1X -' selected. The tooltip says 'To manage groups, see the Location Group'.

Under the 'Coordinated Threat Control' section, there is a note: 'Note that not all enforcer versions and platforms have an IDP module.' Below the note is a checkbox labeled 'Use IDP Module as Sensor' which is currently unchecked. At the bottom left of the form is a 'Save Changes' button.

- Enter the name of the Infranet Enforcer in the **Name** box.
- Enter the password for the SRX enforcer.
- Enter the serial number of the Junos SRX Enforcer. You can view the serial number on the SRX device using the command: `user@host show chassis hardware`
- Ensure that the server certificate for IPS is configured for the interface to which the SRX device is connecting.
- Click **Save Changes**. You must create security policies on the SRX device for traffic enforcement.

Configuring Auth Table Mapping Policies

An auth table consists of username, a set of roles, and IP address of the wired adapter, wireless adapter, or virtual adapter of the user device. Using SRX series firewall you can dynamically create auth table entries when a user tries to access the protected resource. An auth table mapping policy specifies which enforcer device can be used for each user role. These policies prevent the IPS from creating unnecessary auth table entries on all connected enforcer devices.

IPS's default configuration includes only one default auth table mapping policy. When the default auth table mapping policy is enabled, IPS pushes one auth table entry for each authenticated user to all SRX firewalls configured as Infranet Enforcers in IPS.

To configure auth table mapping policies:

1. Select **Endpoint Policy > Infranet Enforcer > Auth Table Mapping**.
2. Select the default auth table mapping policy called **Default Policy** and click **Delete**.

On the New Policy page, do the following:

1. For Name, enter a name to label this auth table mapping policy.
2. (Optional) For Description, enter a description.
3. In the Enforcer section, specify the Infranet Enforcer device(s) to which you want to apply this auth table mapping policy.
4. In the Roles section, specify:
 - Policy applies to ALL roles-To apply this auth table mapping policy to all users.
 - Policy applies to SELECTED roles-To apply this auth table mapping policy only to users who are mapped to roles in the Selected roles list. Be sure to add roles to this list from the Available roles list.
 - Policy applies to all roles OTHER THAN those selected below-To apply this auth table mapping policy to all users except for those who map to the roles in the Selected roles list. Be sure to add roles to this list from the Available roles list.
5. In the Action section, specify auth table mapping rules for the specified Infranet Enforcer device:
 - Always Provision Auth Table-To automatically provision auth table entries for chosen roles on the specified Infranet Enforcer.
 - Provision Auth Table as Needed-To provision auth table entries only when a user with a chosen role attempts to access a resource behind the specified Infranet Enforcer.
 - Never Provision Auth Table-To prevent chosen roles from accessing resources behind the specified Infranet Enforcer.
 - Make sure you delete the Default Policy if you configure any of your own auth table mapping policies. IPS includes this default auth table mapping policy that allows all source IP endpoints to use all Infranet Enforcer devices.
6. If you created a vsys on a ScreenOS Enforcer, enter the ID of the vsys in the vsys text box. To view the enforcers or vsys that are associated with each policy, select Infranet Enforcer > Auth Table

Mapping.

7. Click **Save Changes**.

For more information on dynamic authentication table, see [Configuring Dynamic Auth Table Policies](#)

Configuring Resource Access Policy

A resource access policy specifies which users are allowed or denied access to a set of protected resources. You can specify which users you want to allow or deny by choosing the roles for each resource access policy.

To configure Infranet Enforcer resource access policies:

1. Select **Endpoint Policy > Infranet Enforcer > Resource Access Policy** and click **New Policy**.

On the New Policy page do the following:

2. For Name, enter a name to label this Infranet Enforcer resource access policy.
3. (Optional) For Description, enter a description.

For **Resources**, specify the protocol, IP address, network mask, and port of each resource (or range of addresses) for which this Infranet Enforcer resource access policy applies, one per line. Do not insert any spaces in your entries, or the policy may not be applied correctly.

You cannot specify a host name in a resource access policy. You can specify only an IP address. You can use TCP, UDP, or ICMP.

4. Under Infranet Enforcer, specify the Infranet Enforcer to which this policy applies by using Add.
5. Specify one of the following in the Roles section:
 - **Policy applies to ALL roles**-To apply this Infranet Enforcer resource access policy to all users.
 - **Policy applies to SELECTED roles**-To apply this Infranet Enforcer resource access policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
 - **Policy applies to all roles other than those selected below**- To apply this Infranet Enforcer resource access policy to all users except those who map to the roles in the Selected roles list. You must add roles to this list from the Available roles list.

6. In the Action section, specify whether you want to use this Infranet Enforcer resource access policy to allow or deny access to the specified resources.

If you select deny, a text box is displayed that allows you to customize a deny message for users.

With ScreenOS Enforcer Release 6.3 r13 or later, you can also select Reject Access. The customized deny message is available with the reject action.

The reject action is designed for clients that hang for a long period while waiting for connection initiations that the firewall is blocking. With the deny action, the Enforcer drops traffic in accordance with the IPS policy, but does not send back reject information. The policy action of "reject" denies the traffic and sends a TCP RST to the traffic originator for TCP traffic, or ICMP unreachable for UDP traffic. In earlier versions of ScreenOS and on the Junos Enforcer, the selection of reject results in a deny action.

To record deny actions in the User Access Log, select the **Infranet Enforcer Deny Messages** check box on the **Log/monitoring > User Access > Settings** page. The log records the user, source IP, destination IP, protocol, and destination port.

1. For ScreenOS Enforcers, in the ScreenOS Options section, use the option buttons to select the policy options that you want to apply to selected roles. Use the Add and Remove buttons to specify antispam, logging, IDP, web filtering, antivirus, and deep inspection.
2. By default, all policy options are enabled. To enforce the policies, you must create corresponding policies on the ScreenOS Enforcer. If IPS is upgraded from a previous version, all ScreenOS options are enabled for the resource access policies that were available prior to the upgrade.
3. If you have created a vsys on a ScreenOS Enforcer, enter the ID of the vsys in the VSYS text box, if applicable. The Infranet Enforcer > Resource Access Policy page displays the Enforcers and/or vsys that are associated with each policy.

Configuring SRX Firewall

IPS can utilize a SRX device as a policy enforcement point to work as a Layer 3 Enforcer. When the SRX is configured to work as an enforcer with IPS, the following takes place:

- IPS provisions resource access policies.
- SRX gets the user's role membership information from authentication table entries that are sent by IPS when the user authenticates with the IPS or when the user tries to access resources through SRX.

- SRX does a policy lookup in resource access policies, which is sent by IPS and accordingly takes allow/deny decisions.

For the SRX to perform a IPS policy lookup, the uac-policy application service needs to be turned on in the SRX firewall rule and the firewall rule's action should be set to permit. The SRX security policies have to be manually configured on SRX.

Configuring SRX as an Enforcer

The SRX enforcer works with the IPS device for Layer 3 connectivity. You can connect with source IP or IPsec. For the initial setup, you must specify the IPS device name, IP address, port number over which the Junos Enforcer and IPS device will connect, the interface, the password (the same password as entered on the IPS device), and, optionally, the CA profile and server certificate subject. Use the Junos CLI to add this information.

You can configure the SRX device in "test only" mode. In test only mode, the SRX device does not enforce IPS policies and allows all traffic to pass. However, all policy decisions are logged. This allows you to set up the devices before actual deployment and determine how the IPS solution works using different configuration options. For example, the IPS device and endpoints can reside on different physical interfaces of the Junos Enforcer or on the same interface.

IPS device policies are role based. Each policy specifies a destination (the resources that are being protected), a set of roles, and an action (allow or deny). To determine the roles for users, an auth table maps source IP addresses to roles. When an endpoint accesses the IPS device, the IPS device populates the Junos Enforcer with an auth table entry mapping the endpoint's IP address to the endpoint's set of roles. When evaluating a flow, the source IP address of the initial packet is used to look up the roles. Then the first policy that matches both the destination (resource) and the roles is used to determine whether to permit or deny the flow.

To use IPsec with the SRX device, you must enable IKE services for the gateway. If you have multiple IPsec tunnels with multiple gateways, the hostname for each gateway must be unique.



SRX Series communication to IPS is not supported on an interface that is in a routing instance or VRF instance.

To configure the Junos Enforcer:

1. Set up the trusted interface. The trusted interface connects to the protected resource. The untrusted interface connects to IPS.

2. Ensure that the DHCP server is disabled or enabled as required for the deployment.
3. Create a IPS configuration on the Junos security device, and provide the network information required for connecting using the CLI. This information includes IPS host name, the IP address, and the interface to which the device will connect. The default port for communication with IPS is 11123, you cannot change the port. You must also specify a password, that matches the password configured on IPS.
4. For complete CLI instructions and syntax, see the Junos Software CLI Reference.
 - Specify IPS hostname:
user@host# set services unified-access-control infranet-controller hostname
 - Specify IPS IP address:
user@host# set services unified-access-control infranet-controller hostname address ip-address
 - Specify the Junos interface to which IPS should connect:
user@host# set services unified-access-control infranet-controller hostname interface interface-name
 - Specify the password that the SRX Series or J Series device should use to initiate secure communications with IPS:
user@host# set services unified-access-control infranet-controller hostname password password
5. Set the appropriate timeout and interval values, and specify a timeout action. The timeout that you set specifies the elapsed time beyond which the Junos Enforcer attempts to reconnect with IPS if no communication is received. The interval specifies how often IPS sends a heartbeat to the Junos Enforcer.

6. (Optional) Verify that the certificate of the CA that signed IPS's server certificate is loaded in the Junos Enforcer and that the path to the certificate is specified.



Although certificate verification is optional, there are three different certificate options on the Junos Enforcer that will produce different results.

- If certificate-verification is set to required, it is required that the device verify any IPS server certificate. If any IPS ca-profile is not configured, the commit check fails.
 - If certificate-verification is set to warning (the default), and IPS ca-profile is not configured, the commit check displays a warning about the security risk with a similar warning in the syslog.
 - If certificate-verification is set to optional, there is no warning.
7. Verify routing from IPS to the untrusted interface.
 8. Ensure that both the Junos Enforcer and IPS are set to the correct time. If possible, use a Network Time Protocol (NTP) Server to set the date and time of both appliances.

When you finish configuring IPS instance, the Junos Enforcer can initiate the connection with IPS. The Junos Enforcer optionally validates IPS server certificate if so configured. The device sends the serial number to authenticate with IPS.

For the Junos Enforcer to establish communication, you must configure the Junos Enforcer on IPS.

Configuring Additional TLS Settings

The user can change different SSL/TLS versions and different encryptions in the Outbound SSL Settings.

To change the SSL/TLS versions:

1. Select **Configuration > Security > Outbound SSL Settings** page.
2. Under Outbound Settings, select **TLS 1.2** for maximum security.

- Under Allowed Encryption Strength, select Maximum Security (High Ciphers) for maximum security.

The screenshot shows the configuration page for 'Outbound SSL Options' in the SRX Series Firewall. The breadcrumb trail is 'Configuration > Security > Outbound SSL Options'. The page title is 'Outbound SSL Options'. A navigation bar includes 'Configuration' (with a sub-menu 'Security') and other sections like 'Licensing', 'Pulse One', 'Certificates', 'DMI Agent', 'Sensors', 'Client Types', 'SAML', 'Guest Access', 'Advanced Networking', and 'Notification'. Below this, there are sub-sections: 'Inbound SSL Options', 'Outbound SSL Options' (which is active), 'Health Check Options', 'Miscellaneous', and 'Advanced'. The main content area is divided into several sections: 'DoD Certification Mode' (with 'JITC is Off'), 'SSL NDcPP Mode' (with 'NDcPP is Off'), and 'SSL FIPS Mode' (with 'FIPS is Off'). The 'Outbound Settings' section includes 'Allowed SSL and TLS Version' with a note that the older SSL V2 protocol is no longer supported. It offers four radio button options: 'Use TLS 1.2 (maximize security)' (selected), 'Use TLS 1.1 and later', 'Use TLS 1.0 and later', and 'Use SSL V3 and TLS (maximize compatibility)'. The 'Allowed Encryption Strength' section includes a note to refer to the Admin guide and offers three radio button options: 'Maximize Security (High Ciphers)' (selected), 'Maximize Compatibility (Medium Ciphers)', and 'Custom SSL Cipher Selection'.

Enforcement using EX Series Ethernet Switches

Overview

You can use the EX Series switch as an Infranet Enforcer with IPS. With this solution, IPS is the policy decision point, while the switch is the policy enforcement point. In prior releases, Layer 3 firewalls were the only option for policy enforcement points. This scenario allows enforcement with 802.1X deployments.

To employ the switch as an Infranet Enforcer, you configure a connection between the EX Series switch and the IPS, establish communication, set up 802.1X, configure IPS parameters for admission to the network, and configure resource access policies.

Upon successful configuration, the following occurs:

- The EX Series switch sends a connection request to IPS.
- The EX Series switch shares its RADIUS configuration with IPS from the CLI configuration on the switch.
- IPS creates the RADIUS client for the EX Series switch using the information provided.
- When a user successfully authenticates, IPS provides an auth table entry to the connected EX Series switch. The auth table includes the MAC address of the user, the assigned roles and the port index.
- IPS must receive the attributes Calling Station ID and Network Access Server (NAS) Port from the switch to successfully make the connection.

Configuring EX switch with IPS

The EX Series switch serves as a policy enforcement point. IPS sends auth table entries and resource access policies when an endpoint successfully completes 802.1X authentication or MAC authentication (unmanaged devices). Access for any endpoint is governed by the resource access policies that you configure on IPS. Because resource access policies are employed, firewall filters are not required for the EX Series switch configuration.

Configuring EX switch as an Infranet Enforcer

The EX-series switches will permit or deny network access based on policies developed and distributed by IPS, including those policies based on user authentication status, endpoint posture compliance, user/device role and other policies. The EX-series switches provide standards-based 802.1X port-level access control.

To configure a Juniper EX switch as an Infranet Enforcer in IPS:

1. Select **Endpoint Policy > Infranet Enforcer**.

The screenshot shows the 'Infranet Enforcer > Infranet Enforcer Connection' page. The 'Connection' tab is selected. Below the navigation tabs, there is a description: 'A connection policy specifies the connection between the Pulse Policy Secure and Infranet Enforcer.' There are three buttons: 'New Enforcer...', 'Duplicate...', and 'Delete...'. Below these buttons is a dropdown menu set to '10' records per page and a search box. A table with the following columns is visible: Enforcer, Serial Numbers, Location Group, Platform, Version, FIPS, and IP Address.

2. Click **New Infranet Enforcer** and select **Junos EX** in the **Platform** drop down.

The screenshot shows the 'New Infranet Enforcer' configuration form. The 'Platform' dropdown is set to 'JUNOS EX'. The form includes the following fields:

- Name:** A text input field.
- Password:** A text input field.
- Serial number(s):** A text input field.
- Location Group:** A dropdown menu set to '- No 802.1X -'.

 A 'Save Changes' button is at the bottom. A note at the bottom left states '* indicates required field'.

3. Enter the name of the EX Series switch in the Name box.
4. Enter the password for the **EX Series switch**. This password is a shared secret that administrators of both the switch and IPS can use for connectivity between the two devices.
5. Enter the serial number of the EX Series switch.

6. Select the location group.
7. Click **Save Changes**.

On the EX Series switch, you use the CLI to configure the connection with IPS.

Configuring an Authentication Table

The EX Series switch receives and maintains auth tables for valid user sessions with IPS. An auth tables consist of a unique identification number, the MAC address of the endpoint that initiated the session, and a list of roles that the user has been assigned.

Auth tables are sent from IPS to the EX Series switch when a user is authenticated on the network.



Always Provision and Never Provision Auth table mapping policies are supported for the EX Series switch.

For complete configuration information, see [Configuring Auth Table Mapping Policies](#).

Configuring Resource Access Policy

Using resource access policies with an EX Series switch you can configure authorization for protected resources. If you have configured the EX Series switch as an Infranet Enforcer, select the switch in the resource access policy.

A resource is a single entry in the resource field of the resource access policy. This could be a MAC address, or it could be a combination of IP address ranges, ports, and protocol. A filter term is the access/deny detail for a single resource. The number of terms you can configure per firewall filter will vary, depending on which EX Series switch you are configuring. The below table shows the number of terms allowed per firewall filter for different EX Series switches.

EX Switch	Number of Terms Allowed
EX2200 switch	512
EX3200 and 4200 switches	7,042
EX4500 switch	1,536
EX8200 switch	32,768

EX Switch	Number of Terms Allowed
EX3300 switch	1,436
EX6200 switch	1,400

If you create resource access policies with the number of resources greater than the maximum number of filter terms allowed, the filter is not installed, and 802.1X authentication fails.

For complete information on configuring resource access policy, see [Configuring Resource Access Policy](#).

Enforcement using Screen OS Firewall

Overview

IPS delivers a layer 3 network access control solution when deployed with Screen OS firewall device. The IPS is the policy decision point that determines which users and endpoints can access protected resources. You can use Screen OS firewalls to serve as the enforcement point to provide the ultimate protection to ensure that network assets are secured.

Deployment of IPS using ScreenOS Firewall

This section describes the integration of IPS with ScreenOS firewall. The IPS and Screen OS firewall solution provides functionality for enforcing security policies on a per user and role basis. It also delivers granular level access control so that it can be easily managed through IPS.

Initial Setup

Introduction	User Authentication <input style="width: 100%;" type="text" value="AD"/>		
Use Cases	This server will be used for authenticating end users		
System Settings	MAC Authentication <input style="width: 100%;" type="text" value="ldap"/>		
Switch Configuration	This server will be used for authenticating devices using MAC Address <small>Note: Only LDAP servers can be used</small>		
Profiling	List of available Servers		
Guest Access	Add Server Type <input style="width: 100%;" type="text" value="LDAP"/>		
Enforcement	LDAP Server		
Pulse Connect Secure Configuration	Server Name <input style="width: 100%;" type="text" value="ldap"/>	Host <input style="width: 100%;" type="text" value="10.204.90.216"/>	Server Type <input style="width: 100%;" type="text" value="Active Directory"/>
Authentication Servers	Port <input style="width: 100%;" type="text" value="389"/>	Connection Type <input style="width: 100%;" type="text" value="Unencrypted"/>	Filter <input style="width: 100%;" type="text" value="macAddress=<USER>"/>
Roles	Admin DN <input style="width: 100%;" type="text" value="cn=Administrator,cn=users,dc=u"/>	Password <input style="width: 100%;" type="text" value="*****"/>	Base DN <input style="width: 100%;" type="text" value="OU=MACAddresses,OU=MAC,dc"/>
Compliance Check	Group Filter <input style="width: 100%;" type="text" value="(&(objectClass=group)(cn=*))"/>	Group Member Attribute <input style="width: 100%;" type="text" value="member"/>	Group BaseDN <input style="width: 100%;" type="text" value="OU=MACGroups,OU=MAC,dc=u"/>
Summary	<input type="button" value="Cancel"/> <input type="button" value=" < Previous"/> <input type="button" value=" Next >"/> 		

The authentication process is described below:

1. The endpoint connects to switch to perform the layer 2 authentication with IPS.
2. IPS communicates with authentication server and performs the layer 3 authentication along with host check to ensure that the endpoints meets the corporate policy.
3. The external authentication server such as AD/LDAP confirms the role and sends the entries to IPS.
4. IPS provisions the auth table on ScreenOS firewall with changes in role information if any.
5. The ScreenOS firewall maps the user to a specific resource access policy and then provides the required access.

Configuring IPS with ScreenOS Firewall

The ScreenOS Enforcer connects to IPS over an SSH connection that uses the NetScreen Address Change Notification (NACN) protocol. IPS uses the NACN password and serial number for a connection from the ScreenOS Enforcer. When the ScreenOS Enforcer first turns on, it sends an NACN message containing the NACN password and serial number to IPS. IPS uses the serial number to determine which ScreenOS Enforcer is attempting to connect, and IPS uses the NACN password to authenticate the ScreenOS Enforcer. IPS then begins communicating with the ScreenOS Enforcer using SSH.

Configuring ScreenOS Infranet Enforcer in IPS

To configure a SRX Firewall Infranet Enforcer in IPS:

1. Select **Endpoint Policy > Infranet Enforcer**.

Enforcer	Serial Numbers	Location Group	Platform	Version	FIPS	IP Address

- Click **New Infranet Enforcer** and select ScreenOS Firewall in the **Platform** drop down.

infranet Enforcer > Connection > New Infranet Enforcer

New Infranet Enforcer

▼ Infranet Enforcer

Platform: Platform of this Infranet Enforcer.

* Name: Label to reference this Infranet Enforcer.

* NACN password: NetScreen Address Change Notification password.

* Admin username:

* Admin password:

* Serial number(s): One per line.

Location Group: To manage groups, see the Location Group

▼ Coordinated Threat Control

Note that not all enforcer versions and platforms have an IDP module.

Use IDP Module as Sensor

* indicates required field

- Enter an NACN password for this Infranet Enforcer in the NACN password box. You must enter this same NACN password when configuring the Infranet Enforcer.
- In the appropriate boxes, enter the administrator name and password for signing into the Infranet Enforcer
- Enter the name of the Infranet Enforcer in the **Name** box.
- Enter the password for the ScreenOS enforcer.
- Enter the serial number of the ScreenOS Enforcer. You can view the serial number on the ScreenOS device using the command: **get system**
- Select **No 802.1X** from the Location Group list if you are not using an Infranet Enforcer as an 802.1X RADIUS client.
- Ensure that the server certificate for IPS is configured for the interface to which the SRX device is connecting.
- Click **Save Changes**.

When you finish configuring the Infranet Enforcer, the Infranet Enforcer attempts to connect to IPS. If the connection is successful, a green dot is displayed next to the Infranet Enforcer icon. Under Enforcer Status select **System > Status > Overview**. The Infranet Enforcer IP address is also displayed in **Endpoint Policy > Infranet Enforcer > Connection**.

Configuring Auth Table Mapping Policies

An auth table consists of username, a set of roles, and IP address of the wired adapter, wireless adapter, or virtual adapter of the user device. Using SRX series firewall you can dynamically create auth table entries when a user tries to access the protected resource. An auth table mapping policy specifies which enforcer device can be used for each user role. These policies prevent the IPS from creating unnecessary auth table entries on all connected enforcer devices.

For complete configuration information, see [Configuring Auth Table Mapping Policies](#)

Configuring Resource Access Policy

A resource access policy specifies which users are allowed or denied access to a set of protected resources. You can specify which users you want to allow or deny by choosing the roles for each firewall enforcer access policy.

For complete configuration procedure, see [Configuring Resource Access Policy](#)

Configuring ScreenOS Firewall

IPS can utilize a ScreenOS device as a policy enforcement point to work as a Layer 3 Enforcer. When the ScreenOS device is configured to work as an enforcer with IPS, the following takes place:

- IPS provisions resource access policies.
- Screen OS device gets the user's role membership information from authentication table entries that are sent by IPS when the user authenticates with the IPS or when the user tries to access resources through ScreenOS.
- ScreenOS device does a policy lookup in resource access policies, which is sent by IPS and accordingly takes allow/deny decisions.

Configuring ScreenOS as an Enforcer

You can configure basic Infranet auth Enforcer policies that specify a source zone and a destination zone on the IPS Series device and then push the policies to the ScreenOS Enforcer to add additional policy details, or you can use the ScreenOS Enforcer to configure the policies with the CLI or Web UI. We recommend that you use the IPS Series device to set up the policies for source IP enforcement on the Infranet Enforcer.

Before setting a policy, you must create address book entries for the destination and source addresses unless you use address book entries that already exist, such as Any.

The following example, sets an Infranet auth policy and adds it to the top of the list of policies. The policy allows all traffic of any type from any host to another host. The policy allows traffic according to the Infranet Enforcer resource access policies that you configure on the IPS Series device.

```
set policy top from untrust to trust any permit Infranet-auth
```

The following example sets two address book entries and a policy between them for anyone in the 10.64.0.0/16 range can reach the 10.65.0.0/16 range.

```
set address Trust "10.64 Range" 10.64.0.0 255.255.0.0
set address Untrust "10.65 Range" 10.65.0.0 255.255.0.0
set policy from trust to untrust "10.64 Range" "10.65 Range" any permit Infranet-auth
```

You can use Route mode or Transparent mode to configure a Juniper Networks ScreenOS Enforcer. By default, the ScreenOS Enforcer operates in Route mode. For more information on ScreenOS, see the *ScreenOS Reference Guide*.

Configuring the ScreenOS in Route Mode

The IPS can reside on trust/untrust interface side of the Infranet Enforcer. If IPS resides on the trust interface side, and users come in through the untrust interface, the administrator must configure a policy (untrust to trust) on the Infranet Enforcer that allows traffic to pass between IPS and Pulse Client. By default, Infranet Enforcer traffic from the untrust interface to the trust interface is denied.

The following procedure describes the setup with IPS on the untrust interface side (same side as users).

To configure an Infranet Enforcer in Route mode:

1. Set up the trust interface. The trust interface connects to the protected resource. The untrust interface connects to IPS. Set the following interface (ethernet1/1) settings:
 - Set routing
 - Enable management of the following services:
 - SSL
 - SSH
 - IP (options)
2. Ensure that the DHCP server is disabled or enabled, as appropriate for the deployment.
3. Import the certificate of the CA that signed IPS's server certificate into the Infranet Enforcer.
4. If you set up an NSRP cluster before you import the CA certificate into the Infranet Enforcer, the CA certificate is automatically synchronized to all Infranet Enforcers in the cluster. However, if you set up the NSRP cluster after you import the CA certificate, you must manually synchronize the certificate to the other Infranet Enforcers in the cluster by typing the following CLI command:

```
exec nsrp sync pki
```

You cannot load the self-signed SSL certificate into the Juniper security device.

The certificate of the CA that signed IPS's certificate must be imported on the Infranet Enforcer because the Infranet Enforcer must be able to trust IPS during an SSL session. When a user signs into a server by means of SSL, the server displays a dialog box in which the user can manually accept the certificate that is associated with that server. For the Infranet Enforcer to skip that manual step and automatically accept IPS's certificate, the Infranet Enforcer must have the certificate of the CA that signed IPS's certificate.

5. Create an instance of IPS on the Juniper security device.
6. Enable SSH.
7. Verify routing from IPS to the untrust interface.
8. Ensure that both the Infranet Enforcer and IPS have the correct time. If possible, use a Network Time Protocol (NTP) server to set the date and time of both appliances.

Creating a Route based interface with ScreenOS

When an interface is in route mode, the security device routes traffic between different zones without performing source NAT.

To create a IPS instance on ScreenOS, you must configure the following items:

- IP address or hostname of IPS
- Password to use when the Infranet Enforcer uses NACN to contact IPS
- Source interface
- CA index number (ca-idx)

You can set these items using the Web UI or the CLI.

In the following procedure, you first set interface management options and disable the DHCP server option. Then you enable SSHv2 and configure an IPS server named controller1. Next, you set the host IP address, which is the IP address of the server, to 10.64.12.1. The NACN password is 8!JsP37cK9a*_HiEwe. The NACN password must match the NACN password that you entered for IPS server. The source interface is the interface that the Infranet Enforcer uses to communicate with IPS, and the CA index number is 001.

For this example, the source interface is ethernet 1/1. For a descriptive list of CA index numbers by typing the following command at the ScreenOS CLI:

```
get ssl ca-list
```

To change SSH versions, delete SSH settings by typing the following CLI command:

```
delete ssh device all
```

When you use the Web UI, you do not need to fill in the Full Subject Name of IPS Cert field. If you do fill it in, be sure to enter the entire certificate subject. For example:

```
CN=icl.sample.net,CN=14087306185,CN=06990218,OU=Software,O=Comp,S=CA, C=US
```

To create the instance using the Web UI:

1. Select **Network > Interfaces > Edit > Services** from the left navigation bar to set management options.

2. Select **Network > DHCP > Edit** to disable the DHCP server for both interfaces (Trust and Untrust).
3. Select and load the CA if you have not already done so.
4. Select **Objects > Certificates**.
5. Click **Browse** to find and select the certificate. Then click **Load**.
6. Select **CA** from the show list.
7. Click **Server Settings** and make sure **Check Method** is set correctly for the certificate you are using.
8. Click **OK**.
9. Create IPS instance.
10. Select **Configuration > Infranet Auth > Controllers (List) > New**.
11. Type **controller1** in IPS instance box.
12. Type IP/domain name: **10.64.12.1** in the IP/Domain Name box.
13. For the NACN Parameters, select ethernet1/1 from the Source Interface list.
14. Type **8!JsP37cK9a*_HiEwe** in the Password box.
15. Select the CA from the **Selected CA** list.
16. Enable SSH version 2.
17. Select **Configuration > Admin > Management > Enable SSH (v2)**.

To create the instance using the CLI:

Type the following commands

```
set interface ethernet1/1 manage ssl
set interface ethernet1/1 manage ssh
set interface ethernet1/1 manage ip
set interface ethernet2/1manage ping
set interface ethernet2/1 dhcp server disable
set interface ethernet1/1 dhcp server disable
delete ssh device all
set ssh version v2
```

```
set ssh enable
set infranet controller name controller1 host-name 10.64.12.1
set infranet controller name controller1 password 8!JsP37cK9a*_HiEwe
set infranet controller name controller1 src-interface ethernet1/1
set infranet controller name controller1 ca-idx 001
save
```

Configuring the ScreenOS in Transparent Mode

The ScreenOS device is usually installed between a core router and an access distribution device in a transparent mode. The services are enabled at the zone level, and VLAN1 is used for management.

Transparent mode permits you to implement the following functionality:

- The device can act as a Layer 2 forwarding device, such as a bridge.
- You can control traffic flow between Layer 2 security zones by defining policies.

To configure a ScreenOS Enforcer in Transparent mode:

1. Set up Transparent mode using the predefined security zones, v1-trust and v1-untrust.
2. Assign interfaces to v1-trust and v1-untrust.
3. Configure the IP address for a source interface to establish connectivity with IPS. You can use V1-trust, V1-untrust, or V1-dmz.
4. Configure the broadcast mechanism to flooding (default) or ARP/traceroute. ARP/trace-route is more secure than broadcast.
5. Enable management of the following services for VLAN1:
 - SSL
 - SSH
 - Web (optional)
6. Set up the Juniper Networks security device zones. The protected resources can be in either zone (v1-trust or v1-untrust) as long as the protected resources are in a zone different from the endpoints.
IPS can also reside in either zone. If IPS resides in a zone different from the endpoints, configure a policy that allows traffic to the endpoints through the ScreenOS Enforcer.

7. Import the certificate of the CA that signed IPS's server certificate into the ScreenOS Enforcer. Do not import IPS SSL certificate into the Juniper Networks security device.
8. Create an instance of IPS on the ScreenOS Enforcer.
9. Enable SSH.
10. Verify routing from IPS to the V1-untrust zone.
To use IPsec enforcement with a ScreenOS Enforcer in Transparent mode, you might need to configure a source interface policy on IPS.
11. Ensure that both the Infranet Enforcer and IPS have the correct time. If possible, use a Network Time Protocol (NTP) server to set the date and time of both appliances.

Creating a Transparent Mode instance on the ScreenOS

To create a IPS instance in transparent mode, use the CLI to perform the following actions:

- Assign all interfaces to Layer 2 zones.
- Assign an IP address to vlan1 and set the route command.
- Set interface management options.
- Configure a IPS instance named controller1.
- Set the host IP address, which is the IP address of IPS, to 10.64.12.1.
- Enter the NACN password. The NACN password is 8!JsP37cK9a*_HiEwe. The NACN password must match the NACN password that you entered for IPS.
- The source interface, vlan1, is the interface that the Infranet Enforcer uses to communicate with IPS. The CA index number is 001. For a descriptive list of CA index numbers type the following CLI command: `get ssl ca-list`

You can use the following sample configuration to create the instance using the CLI.



For the firewall to operate in Transparent (Layer 2) mode, all interfaces must be in a Layer 2 zone, such as v1-trust or in the null zone. Interfaces cannot remain in a Layer 3 zone.

```
set interface eth1 zone v1-trust
set interface eth2 zone v1-untrust
set interface vlan1 ip 10.64.12.x
set interface vlan1 route
```

```
set interface vlan1 ip manageable
unset interface vlan1 manage ping
unset interface vlan1 manage telnet
unset interface vlan1 manage snmp
unset interface vlan1 manage web
set infranet controller name controller1 host-name 10.64.12.1
set infranet controller name controller1 password 8!JsP37cK9a*_HiEwe
set infranet controller name controller1 src-interface vlan1
set infranet controller name controller1 ca-idx 0001
```

Verifying the IPS Configuration on ScreenOS Enforcer

You can view the configuration of a IPS instance through the Web UI and the CLI. You can view the following information:

- Name of IPS instance
- IP address or domain name of IPS
- Port number (Default 11122)
- Timeout (60 seconds by default)
- Source interface

The Web UI also allows you to view the NACN password.

Web UI

To view configuration information on the Web UI select the following:

1. **Configuration > Infranet Auth > Controllers** from the left navigation bar.
2. **Configuration > Infranet Auth > General Settings** from the left navigation bar.

CLI

To view configuration information at the CLI, type the following command:

```
get infranet controller name controller1
```

Appendix

Infranet Enforcer Policies Overview

After you set up user roles, authentication servers, realms and sign-in policies, you deploy the Infranet Enforcer in front of servers and resources that you want to protect. You control access through a number of different security policies that you configure on Ivanti Policy Secure.

All policy options are supported on the ScreenOS Enforcer.

Resource access policy-Specifies which users are allowed or denied access to a set of protected resources. You specify which users you want to allow or deny by choosing roles for each resource access policy.

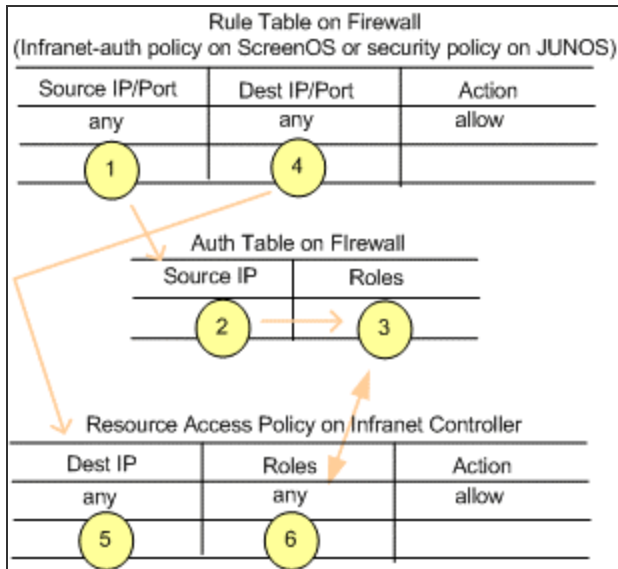
Source IP policy-This is an infranet auth policy the on ScreenOS Enforcer or a security policy on the Junos Enforcer that contains a source and destination that permits the Infranet Enforcer to route clear text traffic between source and destination zones. You can set up a source IP policy on Ivanti Policy Secure and push the policy to the Infranet Enforcer, or you can set up the policy using ScreenOS Web UI or the command line.

Auth table mapping policy-Specifies which Infranet Enforcer device an endpoint must use to access resources when the endpoint is using source IP enforcement. If you are using either a ScreenOS Enforcer with Release 6.1 or later or the Junos Enforcer, you do not need to configure auth table mapping policies. Instead, you can use dynamic auth table provisioning.



You can use a username with spaces, a username with quotation marks, a username with UTF-8 characters, or a username with a backslash (\). Each of these conventions is accepted by the firewall with a valid corresponding auth table entry.

The following figure demonstrates how policies on the Infranet Enforcer and Ivanti Policy Secure interact when a user has an auth table entry on the Infranet Enforcer.



The Infranet Enforcer detects a flow to a specific resource and compares the source IP of the packet with IP addresses in the auth tables. The IP address is associated with a set of roles in the auth table. The destination IP of the packet is matched with the destination IP of a resource access policy to which a set of roles has been assigned. The Infranet Enforcer parses the roles in the resource access policy to determine whether or not the role can access the resource.

Understanding Infranet Enforcer Source IP Security Policies

This topic provides an overview of Infranet Enforcer source IP security policies.

Source IP Security Policy Overview

Source IP enforcement permits users to access resources that are protected by the Infranet Enforcer. IPsec provides an encrypted tunnel for bidirectional traffic, while source IP enforcement allows unencrypted (clear text) traffic between endpoints and the Infranet Enforcer. You can use source IP enforcement alone on the Infranet Enforcer to protect resources alone, or with IPsec on the ScreenOS Enforcer.

To use source IP enforcement, you configure Ivanti Policy Secure policies. On a ScreenOS Enforcer, an Ivanti Policy Secure policy is an infranet auth policy (a policy that includes an infranet-auth statement). On a Junos Enforcer, an Ivanti Policy Secure policy is a security policy (a security policy that includes an application-services Ivanti Policy Secure-policy statement, and may or may not also include a match source-identity statement for user-role firewall functionality).

Ivanti Policy Secure policies control which zones use Infranet Enforcer resource access policies to allow or deny traffic. By default, traffic is denied through the Infranet Enforcer. With Ivanti Policy Secure policies, you control the traffic that is permitted to pass.

When you first set up the Infranet Enforcer and Policy Secure, you bind zones to interfaces. Ivanti Policy Secure policies control the traffic flow between zones. For example, you can configure an Ivanti Policy Secure policy on the ScreenOS Enforcer to enforce traffic from the Untrust zone to the Trust zone. Then, you configure resource access policies and specify resources that are within the Trust zone. The roles that you assign to the resource access policy are permitted to access the specified resources.



Source IP enforcement does not work if there is a NAT device between the endpoint and Ivanti Policy Secure.

In a case where the endpoint is behind a NAT device and Ivanti Policy Secure and the Infranet Enforcer are both on the other side of the NAT device, only one configuration is supported. Source IP enforcement works only with agentless access, and only if it is "one-to-one" NAT, since Ivanti Policy Secure and the Infranet Enforcer both see the external (translated) address, and there will be only one user session per IP address.

Source IP enforcement with agentless access might appear to work, but does not operate properly, if an endpoint is behind a NAT device performing is "many-to-one" NAT. The first user that authenticates from behind the NAT external IP address will get access, but only as long as they are the only authenticated user. If a second user authenticates from behind the same external (translated) IP address, the previous user's session is terminated. The web browser shows that their session was terminated, the same as if an Ivanti Policy Secure administrator deleted their session from the active user table.

If the endpoint is behind a NAT device, Source IP enforcement with Pulse Client does not work at all, regardless of the type of NAT. The agent reports the internal IP address of the endpoint, but the IC will see the external IP of the endpoint. The user can authenticate, and the active user table displays X.X.X.X-Y.Y.Y.Y, where X.X.X.X is the IP address reported by the agent and Y.Y.Y.Y is the IP address detected by the IC. However, no auth table entry will be provisioned to the firewall, since Ivanti Policy Secure detects that the endpoint is behind a NAT.

To provide access for Pulse Client behind a NAT device, you must use the IPsec policy feature. The IPsec enforcement section provides instructions on how to accommodate users in this use case.

ScreenOS Infranet Enforcer Configuration Summary

You can configure Source IP security policies in either of the following ways:

- You can configure basic Source IP policies (source and destination zone) on Ivanti Policy Secure and then push the policies to the ScreenOS Enforcer to add additional policy details. (Recommended)
- You can configure the policies directly on the ScreenOS Enforcer (using the ScreenOS Web UI or CLI).



- To use ScreenOS global policies as infranet auth policies, you must configure them directly on the ScreenOS Enforcer. ScreenOS global policies do not include source and destination zones, and policies pushed from Ivanti Policy Secure must include source and destination zones, so the infranet auth policy pushed by Ivanti Policy Secure is not useful when configuring ScreenOS global policies.
- On ScreenOS, you create a policy using address book entries for the destination and source addresses, as well as policy wildcards, such as Any.

The following example sets an infranet auth policy and adds it to the top of the list of policies controlling traffic from the Untrust zone to the Trust zone. The policy applies to all traffic of any type from any host to another host. The policy allows traffic according to the Infranet Enforcer resource access policies that you configure on Ivanti Policy Secure.

```
set policy top from untrust to trust any permit infranet-auth
```

The following example sets two address book entries and a policy for anyone in the 10.64.0.0/16 range to reach the 10.65.0.0/16 range, subject to resource access policies.

```
set address Trust "10.64 Range" 10.64.0.0 255.255.0.0
set address Untrust "10.65 Range" 10.65.0.0 255.255.0.0
set policy from trust to untrust "10.64 Range" "10.65 Range" any permit infranet-auth
```


Junos Infranet Enforcer Configuration Summary

On the Junos Enforcer, security policies enforce rules for the transit traffic. From the perspective of security policies, traffic enters one security zone and exits another. This combination of a from-zone and a to-zone is called a context on the Junos Enforcer.

A security zone is a logical group of interfaces with identical security requirements. Each security zone contains an address book. Before you can set up policies between two zones, you must define the addresses for each of the zone's address books. A zone's address book must contain entries for the addressable networks and end hosts belonging to the zone.

Each security policy that you create must contain at a minimum match criteria and an action. You can specify additional policy options as required.

You can create security policies on the Junos Enforcer from the Junos Web interface, or from the CLI.

The following example sets an Ivanti Policy Secure-policy security policy controlling traffic from the Untrust zone to the Trust zone. The policy applies to all traffic of any type from any host to another host. The policy allows traffic according to the Infranet Enforcer resource access policies that you configure on Ivanti Policy Secure.

```
set security policies from-zone Untrust to-zone Trust policy ENFORCE_ALL match source-  
address any  
set security policies from-zone Untrust to-zone Trust policy ENFORCE_ALL match  
destination-address any  
set security policies from-zone Untrust to-zone Trust policy ENFORCE_ALL match  
application any  
set security policies from-zone Untrust to-zone Trust policy ENFORCE_ALL then permit  
application-services uac-policy
```

The following example sets two address book entries and a policy for anyone in the 10.64.0.0/16 range to reach the 10.65.0.0/16 range, subject to resource access policies.

```
set security zones security-zone Trust address-book address 10.64_Range 10.64.0.0/16  
set security zones security-zone Untrust address-book address 10.65_Range 10.65.0.0/16  
set security policies from-zone Trust to-zone Untrust policy ENFORCE_ALL match source-  
address 10.64_Range  
set security policies from-zone Trust to-zone Untrust policy ENFORCE_ALL match  
destination-address 10.65_Range  
set security policies from-zone Trust to-zone Untrust policy ENFORCE_ALL match  
application any
```

```
set security policies from-zone Trust to-zone Untrust policy ENFORCE_ALL then permit
application-services uac-policy
```

Understanding Infranet Enforcer Auth Tables

The Infranet Enforcer holds auth tables for valid sessions on Ivanti Policy Secure. Auth tables consist of a unique identification number, the source IP address of the endpoint that initiated the session, the username, and a list of roles that the user has been assigned.

When a user with a username containing spaces or quotes authenticates with Ivanti Policy Secure, the device removes spaces and quotes from the username in the authentication table entry that is sent to Infranet Enforcers.

You can allow the Infranet Enforcer to automatically generate auth tables whenever users are authenticated, or you can configure dynamic auth table allocation. With dynamic auth table allocation, auth tables are provisioned only as a response to a valid request from an authenticated user for a resource behind the Infranet Enforcer.

Dynamic auth table allocation is available on all Junos Enforcers, and on ScreenOS Enforcers with Release 6.1 or later.

Dynamic auth table allocation is required to use IF-MAP Federation.

Understanding Dynamic Auth Table Allocation

You can use the dynamic auth table allocation feature to push auth table entries to the Infranet Enforcer only when a user attempts to access a protected resource. This is more efficient than the Auth Table Mapping Policies option, which requires administrators to provision auth table entries for authenticated users whether they are accessing resources or not. Dynamic auth table allocation reduces auth table entries to only those that are needed, enabling you to deploy smaller firewalls with a larger user population.

When dynamic auth table allocation is used and a user attempts to access a protected resource, the Infranet Enforcer does not yet have an auth table entry for the user, so it sends a drop notification to Ivanti Policy Secure to prompt it to send an auth table entry. Unlike captive portal redirect, which only occurs when the user sends HTTP traffic, drop notifications are triggered by any type of traffic for which the destination is a protected resource.

After the user disconnects, the Infranet Enforcer automatically expires the auth table entry.



On the Junos Enforcer, whenever traffic matches a security policy that includes an application-services uac-policy statement, then the firewall sends a drop notification to Ivanti Policy Secure if there is no auth table entry associated with that traffic. This applies in the captive portal use case, and for all policies that include the application-services uac-policy statement.

However, this behavior changes if user role firewall is configured. When a match source-identity statement is included in any policy within a zone pair (source zone + destination zone), user and role information must be retrieved before policy look-up can proceed. (If all policies in the zone pair are set to match source-identity any, or have no match source-identity state, user and role information is not required and the five standard match criteria are used for policy look-up.) Therefore, for any zone pair in which a security policy is configured that contains a match source-identity statement, the firewall sends a drop notification for all traffic matching that source and destination zone, whether or not the traffic matches the specific security policy containing the match source-identity statement. This can result in an unexpected number of drop notifications if a single zone contains a mix of protected and unprotected resources.

In most deployments, it is recommended that you use dynamic auth table allocation. The benefits of dynamic auth table allocation are based on many factors within the network deployment: the number of Infranet Enforcers, the anticipated number of sessions, and the persistence of user sessions.

The following requirements and limitations apply:

- Dynamic auth table allocation is supported for all deployments with Junos Enforcer and with ScreenOS Enforcers running ScreenOS 6.1 or later.
- Dynamic auth table allocation does not work with HTTP traffic if the captive portal feature is configured to redirect user traffic to an external web server other than Ivanti Policy Secure. Ivanti Policy Secure must be aware of a user login/session before it can provision an auth table entry.
- If you configure dynamic auth table allocation on Ivanti Policy Secure, and the DNS server for the network is behind the Infranet Enforcer, endpoints might occasionally experience DNS time-out issues before resources are provisioned.
- Dynamic auth table allocation is required to use IF-MAP Federation.

One scenario in which static auth tables are more practical is a deployment that forces every endpoint to go through a single Infranet Enforcer for all access. In this case, static auth tables can reduce overall traffic between Ivanti Policy Secure servers and Infranet Enforcers.

For deployments that use static auth table mapping policies (for example, if you are using a ScreenOS Release 6.1 or earlier), we recommend no more than 100 connected Infranet Enforcers. For deployment scenarios with more than 100 Infranet Enforcers, we recommend a deployment strategy using dynamic auth table allocation.

Testing has shown that with 5,000 active sessions, performance is impacted significantly when dynamic auth table allocation is not configured and 100 connected firewalls are deployed.

Performance metrics vary for each Ivanti Policy Secure release.

Configuring Dynamic Auth Table Policies

You can use the dynamic auth table allocation feature to push auth table entries to the Infranet Enforcer only when a user attempts to access a protected resource. This is more efficient than the Auth Table Mapping Policies option, which requires administrators to provision auth table entries for authenticated users whether they are accessing resources or not. Dynamic auth table allocation reduces auth table entries to only those that are needed, enabling you to deploy smaller firewalls with a larger user population.

When dynamic auth table allocation is used and a user attempts to access a protected resource, the Infranet Enforcer does not yet have an auth table entry for the user, so it sends a drop notification to IPS to prompt it to send an auth table entry. Unlike captive portal redirect, which only occurs when the user sends HTTP traffic, drop notifications are triggered by any type of traffic for which the destination is a protected resource.

After the user disconnects, the Infranet Enforcer automatically expires the auth table entry.



On the SRX device, whenever traffic matches a security policy that includes an application-services uac-policy statement, then the firewall sends a drop notification to IPS if there is no auth table entry associated with that traffic. This applies in the captive portal use case, and for all policies that include the application-services uac-policy statement.

However, this behavior changes if user role firewall is configured. When a match source-identity statement is included in any policy within a zone pair (source zone + destination zone), user and role information must be retrieved before policy look-up can proceed. (If all policies in the zone pair are set to match source-identity any, or have no match source-identity state, user and role information is not required and the five standard match criteria are used for policy look-up.) Therefore, for any zone pair in which a security policy is configured that contains a match source-identity statement, the firewall sends a drop notification for all traffic matching that source and destination zone, whether or not the traffic matches the specific security policy containing the match source-identity statement. This can result in an unexpected number of drop notifications if a single zone contains a mix of protected and unprotected resources.

In most deployments, it is recommended that you use dynamic auth table allocation. The benefits of dynamic auth table allocation are based on many factors within the network deployment: the number of Infranet Enforcers, the anticipated number of sessions, and the persistence of user sessions.

The following requirements and limitations apply:

- Dynamic auth table allocation is supported for all deployments with Junos Enforcer and with ScreenOS Enforcers running ScreenOS 6.1 or later.
- Dynamic auth table allocation does not work with HTTP traffic if the captive portal feature is configured to redirect user traffic to an external web server other than IPS. IPS must be aware of a user login/session before it can provision an auth table entry.
- If you configure dynamic auth table allocation on IPS, and the DNS server for the network is behind the Infranet Enforcer, endpoints might occasionally experience DNS time-out issues before resources are provisioned.
- Dynamic auth table allocation is required to use IF-MAP Federation.

One scenario in which static auth tables are more practical is a deployment that forces every endpoint to go through a single Infranet Enforcer for all access. In this case, static auth tables can reduce overall traffic between IPS servers and Infranet Enforcers.

For deployments that use static auth table mapping policies, we recommend not more than 100 connected Infranet Enforcers. For deployment scenarios with more than 100 Infranet Enforcers, we recommend a deployment strategy using dynamic auth table allocation. Testing has shown that with 5,000 active sessions, performance is impacted significantly when dynamic auth table allocation is not configured and 100 connected firewalls are deployed. Performance metrics vary for each IPS release.

To enable dynamic auth table allocation:

1. Select **Infranet Enforcer > Auth Table Mapping** in the admin console. Either delete the Default Policy or specify an Enforcer for which you do not want to configure this feature.
2. Click **Save Changes**.

Binding an Interface to a Security Zone on a Junos Enforcer

Interfaces are the doorways through which traffic enters and exits an Enforcer. Many interfaces share the same security requirements. However, different interfaces can have different security requirements for inbound and outbound data packets. Interfaces with identical security requirements can be grouped together in a single security zone.

A security zone is a collection of network segments that require the regulation of inbound and outbound traffic through policies. Security zones are logical entities to which one or more interfaces are bound. Many types of Enforcers let you define multiple security zones based on network requirements.

You can configure multiple security zones by dividing the network into segments to which you can then apply various security options to satisfy the needs of each segment. At a minimum, you must define two security zones, basically to protect one area of the network from the other. On some security platforms, you can define many security zones, bringing finer granularity to the network security design without deploying multiple security appliances to do so.

From the perspective of security policies, traffic enters one security zone and exits through another security zone. This combination of a "from-zone" and a "to-zone" is defined as a context. Each context contains an ordered list of policies. On the Junos Enforcer, you must define at least two zones to protect one area of the network from another.

You might need to bind the physical interfaces on a Juniper security device to security zones or you might need to change a binding to accommodate your deployment.



Slot numbering varies by platform, and interface numbering varies by module type. For numbering information, see the user guide that accompanied the device for slot and interface numbering information or visit <https://www.ivanti.com/support/product-documentation> to obtain a copy of the user guide specific to your device.

Endpoints must reside in a different security zone from your protected resources. IPS can reside in any security zone. If you place IPS in a different security zone from the one that contains endpoints, you must set a policy allowing traffic from the endpoints to IPS.

Through the policies you define, you can permit traffic between zones to flow in one or both directions. The routes that you define specify the interfaces that traffic from one zone to another must use. Because you can bind multiple interfaces to a zone, the routes you chart are important for directing traffic to the interfaces of your choice.

To view the zones on a Junos Enforcer, type the following command in the CLI:

```
user@host#show security zones
```

To bind the physical interface on the Junos Enforcer, do the following:

- To configure the interface and its IP address for the trust and untrust zones, enter the following statement in Edit mode:

```
user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.168.0.1/24
```

- To configure the trust zone and to assign the interface to it, enter the following statement in Edit mode:

```
user@host# set security zones security-zone trust interfaces interface
```

- To configure the interface and its IP address for the untrust zone, enter the following statement in Edit mode:

```
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.0.0.20/24
```

- To configure the untrust zone and to assign the interface to it, enter the following statement in Edit mode:

```
user@host# set security zones security-zone untrust interfaces interface
```



To use IPsec with the Junos Enforcer, you must enable IKE services for the gateway. If you have multiple IPsec tunnels with multiple gateways, the hostname for each gateway must be unique.

Captive Portal

Captive portal enables an endpoint to be redirected to a specified URL when the user attempts to access a protected resource behind an Infranet Enforcer. The default redirection page is the authentication page of IPS.

The Captive Portal workflow is described below:

1. The user attempts to access a protected resource.
2. The generic source IP policy that matches the destination includes a redirect configuration.
3. The enforcer sends a redirect message to the endpoint browser that includes the URL of IPS.
4. The browser opens a session with IPS and the endpoint completes authentication.
5. IPS sends an authentication table information to Enforcer.
6. IPS redirects the browser back to the original resource.
7. The user tries to access the resource and the enforcer allows the user to access the protected resource.

Configuring Captive Portal

You can configure a captive portal directly on the Infranet enforcer using the CLI. You must create a captive-portal application service and then set the traffic that would like to redirect:

- **unauthenticated**-Select this option if your deployment uses source IP only or a combination of source IP and IPsec. The Infranet Enforcer redirects clear-text traffic from unauthenticated users to the currently connected IPS, or to an IP address or domain name that you specify in a redirect URL.
- **all**-Select this option if your deployment uses IPsec only. The Infranet Enforcer redirects all clear-text traffic to the currently connected IPS, or to an IP address or domain name that you specify in a redirect URL.



- The captive portal feature redirects HTTP traffic only. If the user attempts to access a protected resource using HTTPS or another protocol such as SMTP, the Infranet Enforcer does not redirect the user's traffic. When using HTTPS or another application, the user must manually sign into IPS first before attempting to access protected resources.
 - If there is an HTTP proxy between the endpoint and the Infranet Enforcer, the Infranet Enforcer might not redirect the HTTP traffic.
-

Example: Junos SRX CLI

To use captive portal with the Junos Enforcer, Release 10.2 is required.

To enable captive portal. associate an instance of a captive portal with a security zone use the following command format:


```
user@host# set security policies from-zone zone-name to-zone zone-name policy policy-name
```

To create the captive portal use the following command format:

```
user@host# permit application-services uac-policy captive-portal captive-portal-name
```

You can redirect all traffic, or only unauthenticated traffic on the Junos Enforcer using the following command format:

```
# edit services unified-access-control captive-portal policy redirect-traffic (all | unauthenticated)
```

Example: ScreenOS CLI

To configure a redirect infranet auth policy for deployments that use either source IP only or a combination of source IP and IPsec type the following command:

```
set policy from source-zone to dest-zone src_addr dst_addr any permit infranet-auth redirect-unauthenticated
```

To configure a redirect infranet auth policy for deployments that use IPsec only type the following command:

```
set policy from source-zone to dest-zone src_addr dst_addr any permit infranet-auth redirect-all
```

Creating a Redirect Policy on the Junos Enforcer

In a Junos Enforcer security policy, specify the redirect URL in the following format:

```
user@host# set services unified-access-control captive-portal policy redirect-url url
```

By default, after you configure a captive portal policy, the Junos Enforcer redirects HTTP traffic to the currently connected IPS by using HTTPS. To perform the redirection, the Junos Enforcer uses the IP address or domain name that you specified when you configured IPS instance on the Junos Enforcer.

You specify the redirect URL in a Junos Enforcer security policy using the following hierarchy:

```
user@host# set services unified-access-control captive-portal cap-policy redirect-url "https://%ic-ip%/?target=%dest-url%&enforcer=%enforcer-id%&policy=%policy-id%"
```

These are the four available parameters for redirection.

- target
- enforcer
- policy
- dest-ip

Target, enforcer, and policy are required. Dest-ip is optional. For example:

```
redirect-url "https://acmegizmo.juniper.net/?target=%dest-url%&enforcer=%enforcer-id%&policy=%policy-id%"
```

If you do not specify the redirect URL, the Junos Enforcer uses the default configuration.



To set a redirect URL for the Junos Enforcer, use escape characters instead of dot (.).

For configuration instructions and examples, see the *Junos OS Initial Configuration Guide for Security Devices*.

Creating a Redirect Policy on the ScreenOS Enforcer

From the ScreenOS CLI

- To specify the redirect URL, enter: `set infranet controller name controller1 url "http://10.64.12.1/?target=%dest-url%"`
- To specify the redirect URL without the `?target=%dest-url%` string, enter: `set infranet controller name controller1 url http://abc.company.com`

Deployments with Juniper IDP

About IDP Technology

Securing intranet work application and resource traffic is vital to protecting the network. You can add levels of application security to detect internal threats coming from users who are authenticated through the system by integrating IPS with a Juniper Networks IDP Series sensor.

IPS supports standalone IDP and IDP through the Juniper Networks ISG Series Integrated Security Gateways Infranet Enforcer with the IDP Security Module (supported in ScreenOS Release 6.2 or greater).

The IDP sensor monitors the network on which the IDP system is installed. The sensor's primary task is to detect suspicious and anomalous network traffic based on specific rules defined in IDP rulebases.

The IDP device provides the following types of protection (some of which depend upon the specific configuration):

- Protects against attacks from user to application.
- Detects and blocks most network worms based on software vulnerabilities.
- Detects and blocks non-file-based Trojan Horses.
- Detects and blocks effects of spyware, adware, and key loggers.
- Detects and blocks many types of malware.
- Detects and blocks zero day attacks through the use of anomaly detection.



An IDP Sensor can send logs to one IPS only. However, a IPS device can receive logs from more than one IDP Sensor.

Using the admin console, you can configure and manage interaction attributes between IPS and an IDP, including the following:

- (With standalone IDP) Global configuration parameters such as the IDP hostname or IP address, the TCP port over which the sensor communicates with IPS, and the one-time password IPS and IDP use to authenticate with one another.
 - Various levels of attack severity warnings and the action that IPS takes.
-

The IDP sits within the network and monitors traffic from endpoints that are connected through IPS. You can position the IDP in-line, or you can configure the IDP in sniffer mode.

After IPS connects with the IDP sensor, IPS registers all of the IP addresses to be monitored for potential threats. With standalone IDP, you enter the IP addresses to monitor.

Any abnormal events detected by the IDP Sensor are reported to IPS, which you configure to take appropriate action based on the severity level of the reported events. The IDP Sensor performs reporting functions to allow you to determine what IP address within the network has launched the attacks in addition to any normal logging the IDP has been configured to undertake.

With a large number of connected users IDP can overwhelm IPS with more alert logs than it can process. In this situation, the number of logs sent by the IDP to IPS can be controlled by decreasing the severity level setting in the IDP connection settings.

With IDP deployments using the Infranet Enforcer and the IDP Security Module, the Infranet Enforcer can send messages to Pulse debug log.

IDP Deployment Scenarios Overview

Three possible deployment scenarios are shown in the following figure. The standalone IDP is located within the internal network. All network traffic originating from endpoints that are registered with the IDP is monitored. You can deploy IDP in sniffer mode, or inline mode. You can use transparent mode or route mode with an inline mode configuration. In the first deployment example, the IDP does not monitor IPsec traffic from the user to protected resources.

To monitor all IPsec traffic from users to protected resources, deploy the IDP behind the Infranet Enforcer, as shown in figure.

You can deploy up to ten IDP devices in a network with IPS. Performance is based on how rapidly sessions are created or changed, the number of events that IDP sends to IPS, and the efficiency of the network links that connect the devices. IDP devices must be connected over a high-speed LAN link.

In a clustering environment, only one member of an IPS cluster exchanges information with an IDP sensor. If the connected IPS fails or is shut down, another cluster member will assume the load.

Understanding IPS Deployments with IDP Devices

This topic provides an overview of deployments with IDP devices.

About IDP Devices

The IDP Sensor is a powerful tool to counteract users who initiate attacks. The IDP sensor monitors the network on which the IDP system is installed. The IDP sits within the network and monitors traffic from endpoints that are connected through IPS. You can position the IDP in-line, or you can configure the IDP in sniffer mode. The sensor's primary task is to detect suspicious and anomalous network traffic based on specific rules defined in IDP rulebases.

The IDP device provides the following types of protection (some of which depend upon the specific configuration):

- Protects against attacks from user to application.
- Detects and blocks most network worms based on software vulnerabilities.
- Detects and blocks non-file-based Trojan Horses.
- Detects and blocks effects of spyware, adware, and key loggers.
- Detects and blocks many types of malware.
- Detects and blocks zero day attacks through the use of anomaly detection.

Coordinated Threat Control Overview

In a coordinated threat control deployment, the IDP device reports abnormal events to IPS. The attack logs sent by the IDP device include the source and destination IP addresses and port numbers of the attacking host, and the resource against which the attack was launched, along with the attack identifier, severity of the attack, and the time at which the attack was launched.

IPS displays the attack information received from the IDP sensor on the Active Users page. Based on the attackers IP address and port number, IPS can uniquely identify the user's session.

When you learn that an attack has been launched by an active user, you can disable the user's account, end the user's session, or remediate to a different role. You can choose automatic or manual actions for attacks detected by the IDP sensor. For manual action, you look up the information available on the Active Users page and decide on an action. For automatic action, you configure the action in advance when you define IDP policies.

IPS displays an error message to the user whose account has been disabled indicating the reason.

Deployments with IDP Series Devices

You can deploy IPS with IDP Series devices in coordinated threat control deployments and user-role-based IDP policy deployments. User-role-based IDP policy deployments require IDP Series 5.0 or later. To display the version of an associated IDP device in IPS admin console, select **System > Configuration > Sensors**.



An IDP Sensor can send logs to one IPS only. However, IPS can receive logs from more than one IDP Sensor.

Using the admin console, you can configure and manage interaction attributes between IPS and an IDP Series device, including the following:

- Global configuration parameters such as the IDP hostname or IP address, the TCP port over which the sensor communicates with IPS, and the one-time password IPS and IDP use to authenticate with one another.
- Various levels of attack severity warnings and the action that IPS takes
- IP addresses to monitor.

With a large number of connected users IDP can overwhelm IPS with more alert logs than it can process. In this situation, the number of logs sent by the IDP to IPS can be controlled by decreasing the severity level setting in the IDP connection settings.

Deployments with IDP-Enabled Infranet Enforcers

IPS also supports IDP through the Juniper Networks ISG Series Integrated Security Gateways Infranet Enforcer with the IDP Security Module (supported in ScreenOS Release 6.2 or later).

Unlike a standalone IDP which requires manual configuration on the IDP to allow communication with the IPS, the ScreenOS Enforcer or the Junos Enforcer use the existing communication channel with IPS.

If you are using integrated IDP with the ISG-1000 or ISG-2000, see, https://www.juniper.net/techpubs/en_US/release-independent/screenos/information-products/pathway-pages/screenos/product/index.html. If you are using Junos IDP with Junos OS Release 10.0, see *Junos OS Initial Configuration Guide for Security Devices*. ISG-IDP and CTC are configured the same on IPS.

When ISG-IDP or Junos IDP are activated, ScreenOS or Junos notifies IPS when an attack event is detected from any endpoint. To avoid overwhelming the SSH connection between IPS and the Infranet Enforcer, the number of attack notifications is limited to ten per second. If additional attacks are detected, the Infranet Enforcer holds an additional ten notifications in a queue.

ISG-IDP or Junos devices attached to any node in a cluster may send messages regarding sessions attached to any node in the cluster.

There is a Use IDP module as Sensor check box on the Infranet Enforcer admin console page. If you select the check box and there is no IDP module or if the Enforcer is not running a compatible version, IPS logs an appropriate message.

With IDP deployments using the Infranet Enforcer and the IDP Security Module, the Infranet Enforcer can send messages to Pulse debug log.

Monitoring IDP-Reported Events

After the IDP Sensor has been set up, you can specify the events you want the IDP to watch for and the actions that Ivanti Policy Secure takes once a particular event has been noted and reported.

In two locations on Ivanti Policy Secure, you can specify actions to be taken in response to users that perform attacks:

- **Sensor Event policies page**—Define the policy on this page to generate an automatic response to users who perform attacks.
- **Users page**—Manually identify and quarantine or disable users on the Active Users page, which lists users who have performed attacks.

Activating IDP for the ScreenOS or Junos Enforcer

To activate ISG-IDP or Junos IDP on Ivanti Policy Secure:

1. Select **Ivanti Policy Secure > Infranet Enforcer**.
2. Select the name of the Enforcer on which you want to activate IDP.
3. Select the **Use IDP Module as Sensor** check box. Additional options are presented.
4. Select **For sessions provisioned for this Enforcer only to limit** monitored sessions to this device. This is applicable in an IF-MAP Federation network.

5. Select **1 - INFO through 5 - Critical** from the Severity menu. The severity filter allows you to specify the level of attacks that the Infranet Enforcer reports to Ivanti Policy Secure. For example, if you select 3, only level 3 attacks or higher are reported.

Managing Interoperation with IDP Devices

The Sensors tab allows you to specify the system settings Ivanti Policy Secure uses to establish a connection to an IDP device. Select **System > Configuration > Sensors > Sensors**. The main Sensor page displays the sensor, the network address, the state (enabled), the version, and the status of any configured sensors. The following sections describe tasks related to configuring and managing interaction between Ivanti Policy Secure and an IDP Sensor:

Configuring Communication with an IDP Device

To configure communication with an IDP device and a IDP log monitoring policy:




To use the IDP sensor with Ivanti Policy Secure you must enable logging for the applicable policies.

1. Select **System > Configuration > Sensors**.
2. Click **New Sensor**. The admin console displays the New Sensor page.
3. Under Sensor Properties, specify the following information:
 - **Name**—A name Ivanti Policy Secure uses to identify the new connection entry.
 - **Hostname**—The hostname or IP address of the IDP Sensor to which Ivanti Policy Secure connects in order to receive application and resource attack alert messages.
 - **Port**—The TCP port on the IDP Sensor to which IPS listens when receiving application and resource attack alert messages.
 - **One-time password**—The encrypted password IPS uses when conducting the initial Transport Layer Security (TLS) handshake with the IDP Sensor. You must enter the encrypted IPS OTP password as displayed on the IDP ACM configuration summary screen.



The hostname, TCP port, and one-time password must already be configured on the IDP Sensor before this configuration can be successful.

4. Under **Monitoring Options**, specify IP addresses to monitor and the minimum alert severity level the IDP Sensor records and submits to IPS:
 - In the Addresses to Monitor field, specify individual IP addresses and address ranges, one entry per line. IDP reports attack information only for the IP addresses that you specify. For IDP to report all events to IPS, enter 0.0.0.0/0. For IDP to report only selected events, enter <default> to permit IDP to report events for events with source IPs that have an active user session on IPS, and /or enter one or more addresses or address ranges for any endpoint that you want the IDP sensor to report.

 With ISG-IDP or Junos IDP, you do not need to specify which IP addresses to monitor. The Infranet Enforcer monitors all IP address for which auth tables exist.

 - Select one of the severity options available in the Severity filter drop down list. The severity level is a number on a scale from 1 to 5, where 1 is informational and 5 is critical. This option represents the severity of messages the IDP should send to IPS.
5. Click **Save Changes**.

Enabling or Disabling IDP Sensors

To enable or disable existing IDP Sensor entries on IPS:

1. Select **System > Configuration > Sensors**.
2. Select the check box for one or more IDP Sensor entries to enable or disable.
3. Click **Enable** or **Disable** to enable or disable the specified IDP Sensor entries, respectively.

Reconnecting to an IDP Sensor

When the connection to an IDP Sensor is down, you can use the admin console on IPS to re-establish the connection. You can also use the admin console to refresh the status of existing connections between IPS and the IDP Sensor.

To re-establish communication with an IDP Sensor, you must generate a new One-time Password.

To reconnect to an associated IDP Sensor:

1. Select the check box next to the IDP Sensor to which you want to reconnect.
2. Click **Reconnect**.
The admin console displays a message indicating that IPS is currently attempting to re-establish connection to the specified IDP Sensor. This page automatically refreshes each second during the reconnection process. Otherwise, the connection status page automatically refreshes once every 30 seconds.

Refreshing and Displaying the Connection Status

To refresh and display the connection status for the specified IDP Sensor:

1. Select the check box for one or more IDP Sensor entries to display current connection status.
2. Click **Refresh**.

Deleting an IDP Sensor Entry

You can delete existing IDP Sensor entries that define a connection between IPS and an IDP Sensor.

To delete one or more existing IDP Sensor entries from IPS:

1. Select the check box for the IDP Sensor entry or entries to delete.
2. Click **Delete**, then confirm that you want to delete the sensor entry or entries.

Identifying and Managing Quarantined Users Manually

When IPS quarantines a user based on an attack, you can display and manage the states by locating the user link in the **Active Users** page.

- A small warning icon is displayed in front of the username.
- The linked username.
- An enabled Quarantined option button on the specific user's page. If the user is not quarantined, the option button is disabled.

To manage quarantined users:

1. Locate Identify quarantined users at **System > Status > Active Users**.
2. The quarantined user and click on the username link. The user page opens, showing a number of options.
3. Click **Disabled** to disallow a user from authenticating.
4. Click **Quarantined** to leave a user in a quarantined state. The Quarantined option is enabled only if the user is already quarantined.



IPS assigns quarantined users to the quarantined role, regardless of their log in realm.

5. Click **Save Changes**.

To re-enable previously quarantined or disabled users, select Authentication > Auth. Servers > Select Server > Users and click the link for the given user.



You can also disable users from this location.

6. Click **Enabled** to release the user from quarantine.
7. Click **Save Changes**.

All Sensor events are logged at **System > Log/Monitoring > Sensors > Log**.

Using Role-Based Policies to Monitor User Activity

If you are using IDP Release 5.0 or later or ScreenOS ISG-IDP Release 6.3 or later, you can add enhanced user management capabilities to your IPS IDP deployment. This feature is supported for endpoints using Pulse Client and users who connect with agentless access.

When a user session is established on IPS, IPS pushes session information including IP address, username and the roles to which the user is assigned to the IDP. The session information allows IDP to apply policies based on user roles, or on the username which is added to the IDP log.

Since role selection for a user can be based on the results of Host Checker policies, you can set policies that are based on Host Checker results. For example, if a user is assigned to a restrictive role based on the results of a Host Checker policy requiring an instant messaging software patch, you can restrict instant messenger traffic for that role.

IPS keeps the IDP device updated when a user's role changes or when a session is deleted. IDP's application policy enforcement reflects the most currently available information about a user.

If role-based policies are less restrictive than IP address based policies, some users could be inadvertently blocked during this period. Once session information is obtained about the endpoint IDP re-evaluates the endpoint and applies the less restrictive policies.

If role-based policies are more restrictive than IP address based policies, IDP cannot apply the more restrictive policies, and an endpoint could engage in potentially damaging behavior prior to session information being sent.

If you are using IPS and IDP in a network that employs IF-MAP client and server Federation, and IDP detects an attack that is attributed to a session, IDP informs IPS about the attack. Upon notification, IPS publishes the information to any attached IF-MAP servers. The IF-MAP server notifies IPS that originally published the session and IPS takes the appropriate action based on the applicable Sensor Event Policies.

Provisioning ICS sessions to PAN/Check Point/FortiGate Firewall

Overview

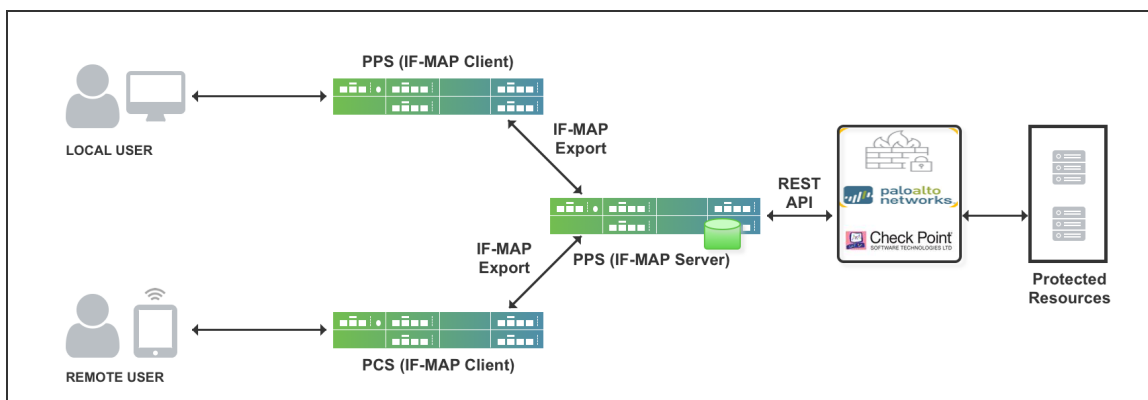
Ivanti Policy Secure (IPS) integrates with Palo Alto Network's (PAN)/Check Point/ FortiGate Next Generation Firewall to provision user's identity information (user name, roles and IP address) to PAN/Check Point/ FortiGate firewall.

This section focuses on provisioning Ivanti Connect Secure(ICS) /IPS user's identity information to PAN/Check Point/ FortiGate firewall using IF-MAP server. Using this solution access control can be provided for ICS/IPS users for accessing resources protected by Firewall.

Deployment of IPS/ICS using PAN/Check Point/ FortiGate Next Generation Firewall

In a federated enterprise, a user can log in to a IPS or ICS device (remote access) for authentication and access the resource protected by the PAN/Check Point/ FortiGate Firewall. The session information is shared across IPS or ICS device using IF-MAP protocol through IF-MAP server.

The PAN/Check Point/ FortiGate Firewall controls the IPS and ICS user's access to protected resources based on the policy settings. The IF-MAP server receives the session information of multiple IPS and ICS and provisions user identity information to Firewall. The federation requires provisioning of user's information on the PAN/Check Point/ FortiGate Firewall and allows access to the protected resource based on the resource access policies that are configured on IPS.



The authentication process is described below:

1. The remote user establishes VPN tunnel using Pulse Client and the role is granted to the user based on policy configured on ICS.
 - ICS session is exported to IF-MAP server.
 - IF-MAP server provisions user identity details to PAN/Check Point/ FortiGate Firewall.
2. The remote user tries to access PAN firewall protected resource. PAN/Check Point/ FortiGate Firewall allows access to protected resource if the user is authorized.
3. User's role changes while logged in (for example, when Host Check compliance change causes role(s) to change). In this case, user's new role(s) are sent to PAN/Check Point/ FortiGate Firewall.
4. User logs out of ICS. In this case, all information associated with the user from that endpoint is removed from the Firewall. User is denied access to protected resources by Firewall.



The same workflow applies to local users connecting through IPS.

IF-MAP Configuration

A high-level overview of the configuration steps needed to set up and run the integration:

- The Administrator configures IF-MAP clients (IPS, ICS) on IF-MAP server admin UI from System > IF-MAP Federation.
- Install the Device certificates and Trusted Server CA from System > Configuration > certificates on both IF-MAP Server and IF-MAP client.
- From IF-MAP Server admin UI, admin configures PAN Firewall device by entering the following:
 - Name for the PAN/Check Point/ FortiGate Firewall
 - IP address of the PAN/Check Point/ FortiGate Firewall
 - API Key for PAN/ Shared Secret for Check Point/ FortiGate
- Administrator configures the Infranet Enforcer Auth Table Mapping Policies.

When the IPS or ICS session is exported to IF-MAP server, IF-MAP server provisions user identity details to configured PAN/Check Point/ FortiGate Firewall based on the configured Auth Table Mapping Policies.

Step1: Configuring IF-MAP Server

To configure IF-MAP server on the IPS:

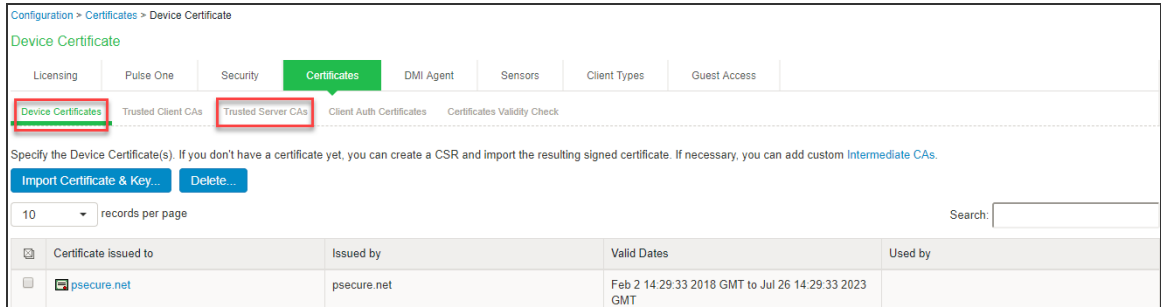
1. Select **System > IF-MAP Federation > Overview**.
2. Select **IF-MAP Server**.
3. Click **Save Changes**.

The screenshot shows the 'IF-MAP > Overview' configuration page. It has three tabs: 'Overview' (selected), 'This Server', and 'This Client'. Below the tabs is a descriptive paragraph about IF-MAP federation. A yellow warning banner states: 'Warning: Please reduce total log file sizes to 500 MB, under Log/Monitoring and Troubleshooting, to ensure enough space for the IF-MAP database.' Below the warning, there are radio buttons for 'IF-MAP Server' (selected), 'IF-MAP Client', and 'No IF-MAP'. There is also a checkbox for 'Enhance IF-MAP Server storage'. A 'Save Changes' button is at the bottom left.

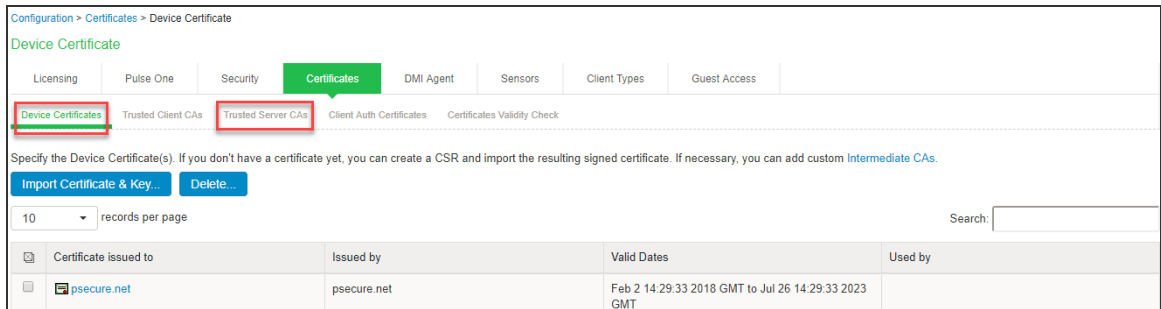
4. Select **IF-MAP > This Server > Clients > New Client** and add **IPS/ICS as IF-MAP client**.

The screenshot shows the 'IF-MAP > This Server > Clients > New IF-MAP Clients' configuration page. It has a section for 'New IF-MAP Clients' with a sub-section 'IF MAP client'. There are three text input fields: 'Name' (with a note 'Label to reference this IF-MAP client'), 'Description', and 'IP addresses' (with a note 'All possible source IP addresses for inbound connections from the client'). Below these is an 'Authentication' section with radio buttons for 'Basic' and 'Certificate'. A 'Save Changes' button is at the bottom.

5. Install the Device certificates and Trusted Server CA from **System > Configuration > certificates** on both IF-MAP Server.



6. If the client is added successfully the status turns to green color.



Step 2: Configuring IF-MAP Client

To configure the IF-MAP client:

1. Select **System > IF-MAP Federation > Overview**.
2. Select **IF-MAP Client**.

3. Enter the IF-MAP server IP address or the complete server URL.

After completing the IF-MAP server and IF-client configurations, configure the IF-MAP Policies. For more information, see *Configuring Session Export Policies*

i This use case supports configuring only Session-Export policies.

Step 3: Viewing the Federated Session Details

To view the federated session details, select **System > IF-MAP > This Server > Federation-wide Sessions**.

User	Capabilities	IF-MAP Roles	Device Attributes	Signin Time	Events	Signed in IP Address	Signed in MAC Address	Publisher ID
user1	LimitedAccess_Role			2018-01-12 09:37:40		10.000.110.5		1CsxZsQ/PCS-90.250

Visibility based Firewall Enforcement

Overview

Profiler provides visibility of the endpoints connected to network. On Profiler, Profile groups can be created using an attribute or combination of device attributes.

The profiler discovered and classified devices with matching attributes belong to configured groups. In few customer environments such as manufacturing industries devices should be able to access applications/resources protected by firewall.

In such scenarios, IPS allows Administrator to provision Auth Table Mapping policy and Resource Access policy configured using profile groups for the devices. IPS provisions the device identity information to the firewall and then Administrator can configure firewall policy based on the requirement.

The provisioning of device information to firewall is described below:

1. Profiler configured on IPS discovers devices connected to network.
2. IPS gets the profiled device information, which belongs to one or more groups. IPS then uses this device information to provision Auth Table Mapping to firewall. The Auth Table Mapping policy defines Profile Group based access control to firewall protected devices.
3. Device Identity details (user id: MAC address of the device, IP address and Profile Group Name) are provisioned to firewall.
4. Device tries to access resources protected by firewall. Devices are allowed to access resources behind firewall based on Profile Group.
5. Any change to Profile Group information for a device will be updated in the firewall.



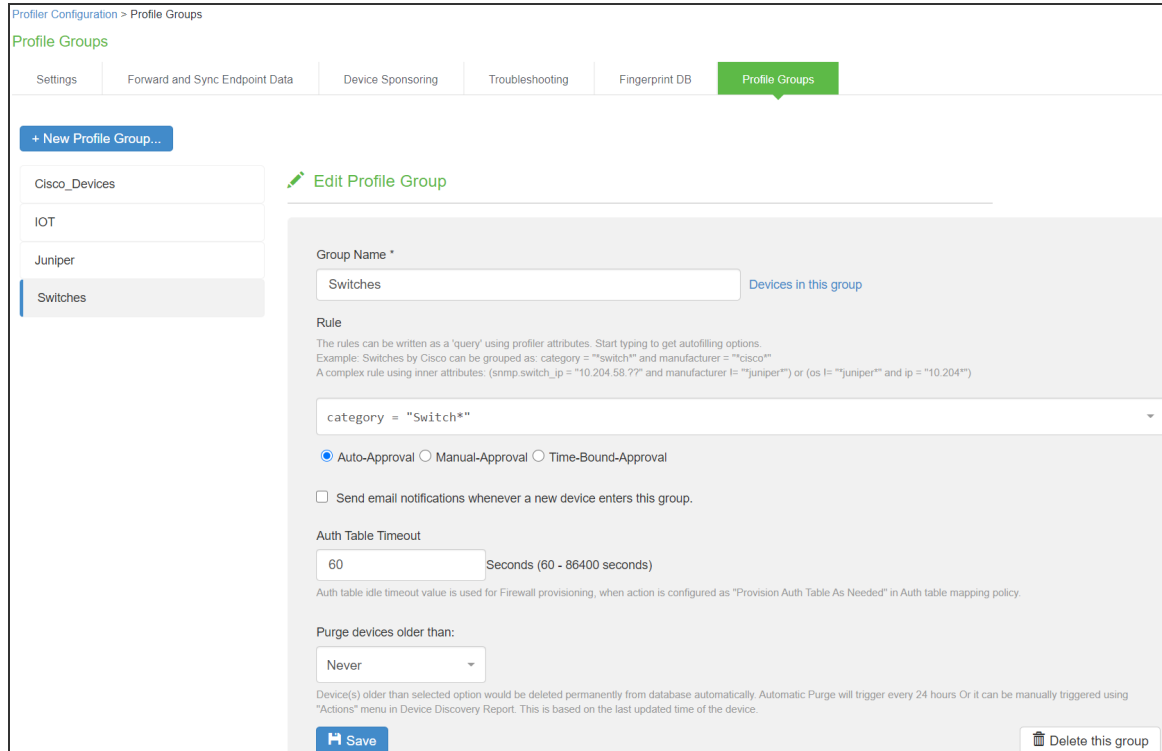
- SRX security policy applies to the role ID and not the role name. Hence, IPS exports Profile group IDs to SRX and not the Profile group names.

- Resource access policy and IoT policy configured based on Profile groups will be exported to firewall along with group information.

Configuring Firewall Provisioning based on Profile Group

To configure firewall provisioning based on Profile group:

1. Admin configures local profiler on IPS to discover devices connected to network. For Profile group configuration, see [Configuring Profiler Groups](#). Auth Table Timeout option is used for dynamic auth table policy provisioning to firewall (Applies only to SRX firewall).



2. Configure firewall as an Enforcer, select **Endpoint Policy > Infranet Enforcer > Connection** and add the enforcer.
3. Configure Auth Table Mapping Policy based on Profile Group, select **Endpoint Policy > Infranet Enforcer > Auth Table Mapping**. Under Provision Settings, enable **Provision Auth Table based on Profile Groups**.

4. Select the Profile Group to which the policy applies and click Add and then click Save Changes.

Infranet Enforcer > Infranet Enforcer Auth Table Mapping Policies > New Policy

New Policy

* Name: Required: Label to reference this policy

Description:

▼ Infranet Enforcer

Specify the Infranet Enforcer(s) to which this policy applies.

Available Enforcers: Add -> Remove

Selected Enforcers:

▼ Enforcement Settings

Enable this option to provision only IP-User mapping to Palo Alto Networks Enforcer. Applicable to Palo Alto Networks Enforcer only.

Provision only IP-User mapping to Palo Alto Networks Enforcer

▼ Provision Settings

Enable this option to provision Auth Table based on Profile groups (for devices that require resource access without authentication).

Provision Auth Table Based on Profile groups

▼ Profile Group

Select the profile group(s) for which this policy applies.

Available Profile Group(s):
 Add -> <- Remove

Selected Profile Group(s):

▼ Actions

Always Provision Auth Table

Provision Auth Table As Needed Only available for Juniper enforcers.

Never Provision Auth Table

VSYS:

▼ One-to-one NAT Deployment

Provision Auth table for one-to-one NAT Deployment Enable this option to provision Auth Table for one-to-one NAT Deployment.

Save Changes Save as Copy

5. Configure Resource Access Policy based on Profile Group, select **Endpoint Policy > Infranet Enforcer > Resource Access Policy**. Under Provision Settings, enable **Provision Resource Access Policy based on Profile Groups**.

6. Select the Profile Group to which the policy applies and click Add and then click Save Changes.

Infranet Enforcer > Infranet Enforcer Resource Access Policies > RESOURCE_ACCESS_JUNOS_SWITCHES

RESOURCE_ACCESS_JUNOS_SWITCHES

General

* Name: RESOURCE_ACCESS_JUNOS_SWITCHES Required: Label to reference this policy.

Description:

Infranet Enforcer

Platform: Juniper Enforcers Palo Alto Networks Firewall

Specify the Infranet Enforcer(s) to which this policy applies.
(Applicable for only Juniper and Palo Alto Networks Firewalls.)

Available Enforcers: Selected Enforcers:

Add ->
Remove

SRX (SRX)

Resources

Specify the resources for which this policy applies, one per line.

* Resources: 10.10.10.0/24.*
20.20.10.0/20.*

Examples:
tcp://*.1-1024
tcp://*.80,443
udp://10.10.10.0/24.*
icmp://10.10.10.10/255.255.255.255
10.10.10.0/24

Provision Settings

Enable this option to provision Resource Access policies based on Profile groups (for devices that require resource access without authentication).

Provision Resource Access Policy Based on Profile groups

Profile Group

Select the profile group(s) for which this policy applies.

Available Profile Group(s): Selected Profile Group(s):

CISCO
juniper

Add ->
<- Remove

IOT
Switches

Actions

Allow access
 Deny access

Enforcer Options

Specify the Enforcer options that should be enabled. If enabled here, the option must also be specified on the Enforcer policy that controls UAC traffic in order to take effect.

ALL Enforcer Options
 SELECTED Enforcer Options
 Enforcer Options OTHER THAN those selected below

Available options: Selected options:

Antispam
Logging
IDP
Web Filtering
Antivirus

Add ->
Remove

(none)

VSYS:

NOTE: changes to this page will cause a slight interruption of service for Infranet Enforcer Resource Policies users.

Save Changes Save as Copy

* indicates required field

7. For IoT access policy, select **Endpoint Policy > IoT Access > Enforcer Policy Configuration**.
Under Provision Settings, enable **Provision Resource Access Policy based on Profile Groups**.

IoT Access > IoT Policy Provisioning > Enforcer Policy Configuration > New Policy

New Policy

* Name: Required: Label to reference this policy.

Description:

▼ Infranet Enforcer

Platform: JUNOS SRX Palo Alto Networks Firewall

Specify the Infranet Enforcer(s) to which this policy applies.
(Applicable for only Juniper and Palo Alto Networks Firewalls.)

Available Enforcers: Selected Enforcers:

▼ Security Zones

Specify firewall security zones for this policy.
If security zone is not specified, then it applies to all zones i.e. any. Multiple zones can be specified with comma separated. Example: trust,mgmt

Source Zone: Destination Zone:

▼ Device Details

Specify the filter for getting resources.

Category and Manufacturer Profile Group

[Click here](#) to configure Device Category or Profile Group.
Select the profile_group(s) for which this policy applies.

Available Profile Group(s): Selected Profile Group(s):

Service:

Auto-Update Newly Discovered Devices.

▼ Resources

Resources will be auto-populated using the configuration specified in Device Details panel, port field is editable.
Policy for the selected resources will be pushed to enforcer.

10 records per page Search:

IP	Protocol	Port	<input type="checkbox"/>
10.25.15.150		<input type="text"/>	<input checked="" type="checkbox"/>
10.25.15.250		<input type="text"/>	<input checked="" type="checkbox"/>
10.25.15.251		<input type="text"/>	<input checked="" type="checkbox"/>
10.25.15.252		<input type="text"/>	<input checked="" type="checkbox"/>
10.25.15.253		<input type="text"/>	<input checked="" type="checkbox"/>
10.96.195.224		<input type="text"/>	<input checked="" type="checkbox"/>

Showing 1 to 6 of 6 entries

▼ Provision Settings

Enable this option to provision Resource Access policies based on Profile groups (for devices that require resource access without authentication).

Provision Resource Access Policy Based on Profile groups

▼ Profile Group

Select the profile_group(s) for which this policy applies.

Available Profile Group(s): Selected Profile Group(s):

▼ Actions

Allow access Deny access

▼ Enforcer Options

VSYS:

NOTE: changes to this page will cause a slight interruption of service for Infranet Enforcer Resource Policies users.

IoT Access > IoT Policy Provisioning - Enforcer Policy Configuration

IoT Policy Provisioning - Enforcer Policy Configuration

IoT Policy Provisioning

Basic Configuration Enforcer Policy Report **Enforcer Policy Configuration** Device Configuration

Show policies that apply to Enforcer: All Enforcers

Showing 1 to 5 of 5 entries records per page Search:

<input type="checkbox"/>	Policy	Category	Manufacturers	Resource Profile Groups	Auto-Update	Enforcers	Roles	Source Profile Groups	Resources	Action
<input type="checkbox"/>	RESOURCE_ACCESS_PAN_IoT			IOT	ON	PAN (PAN)	NA	IOT	10.25.15.150:* 10.25.15.250:* 10.25.15.251:* 10.25.15.252:* 10.25.15.253:* 10.96.195.224:*	Allow

- If there are Auth Table Mapping Policies based on Roles as well as Profile Groups and if there is an authenticated session for an endpoint which is also profiled and belongs to group(s), then user roles will be given precedence over profiler groups for firewall provisioning.
- If the user is logged out but profiled information is still available in the Profiler database then endpoint information will not be provisioned to firewall based on profile groups. However, it will be synced with firewall during next reconciliation.
- If there is an authenticated session and if the Auth Table Mapping policy provisioning is changed to groups from roles then the corresponding entry may get deleted from the firewall if there are no other policies applying to the user role(s).



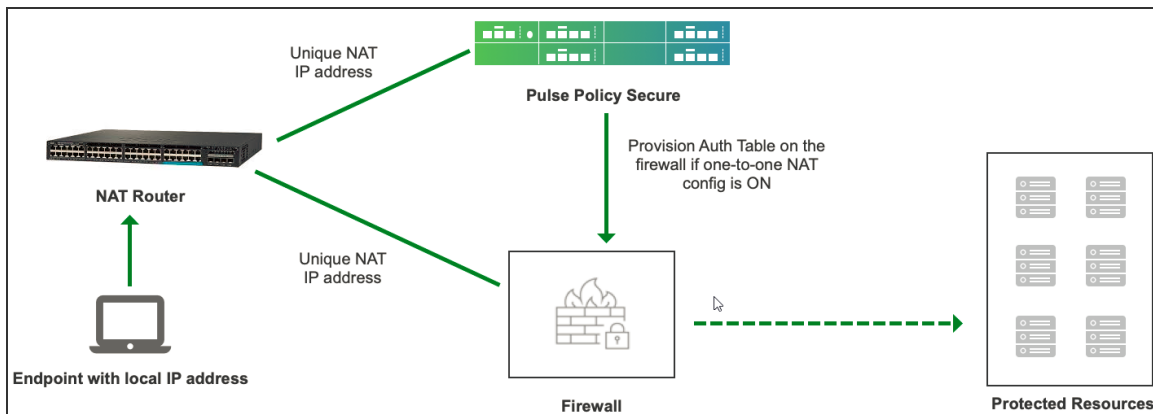
One-to-One Network Address Translation

Overview

One-to-One NAT is the process that maps one internal private IP address to one external public IP address. This helps to protect the private IP addresses from any malicious attack or discovery as the private IP addresses are kept hidden. IPS allows admin to provision auth table entries for endpoints behind one-to-one NAT deployment.

One-to-One NAT Deployment

In this deployment, each end user is having their local address and they are assigned a unique NAT IP address. IPS labels the end user as behind NAT for this type of deployment. The resources are provisioned to firewall only if the Provision Auth table for endpoints behind one-to-one NAT deployment option is enabled on IPS.



The authentication process is described below:

1. User behind one-to-one NAT logs in and the corresponding user role is assigned.
2. A matching auth table mapping policy is detected. If configuration for **Provision Auth table for one-to-one NAT Deployment** option is enabled in this policy, then authentication table for external public IP address for the user is pushed on the firewall.
3. User logs out and all the external public IP address information associated with the user from that endpoint is removed from the firewall.

Configuring one-to-one NAT

To configure one-to-one NAT on IPS:

1. Select **Endpoint Policy > Infranet Enforcer > Auth Table Mapping**.

2. Under One-One NAT deployment, enable the checkbox for **Provision Auth Table** for one-to-one NAT deployment.

Infranet Enforcer > Infranet Enforcer Auth Table Mapping Policies > AUTH PROV

AUTH PROV

* Name:

Description:

▼ Infranet Enforcer

Specify the Infranet Enforcer(s) to which this policy applies.

Available Enforcers:

Selected Enforcers:

▼ Roles

Policy applies to ALL roles
 Policy applies to SELECTED roles
 Policy applies to all roles OTHER THAN those selected below

Available roles:

Selected roles:

▼ Actions

Always Provision Auth Table
 Provision Auth Table As Needed Only available for Juniper enforcers.
 Never Provision Auth Table

VSYS:

▼ One-to-one NAT Deployment

Provision Auth table for one-to-one NAT Deployment Enable this option to provision Auth Table for one-to-one NAT Deployment.

* Indicates required field

3. The Admin is redirected to a confirmation page with a warning message.



This configuration option is recommended to use for one-to-one NAT Deployment. It is not recommended to use for many-to-one NAT Deployment. If used, it could allow multiple endpoints behind many-to-one NAT to access resources without authentication.

4. Click **Enable**.
5. Click **Save Changes**.

IF-MAP Federation

Overview

The federation allows users to connect to a IPS or ICS appliance and then access resources that are protected by the firewall connected to different IPS without re-authentication. For example, users in large campus sites and in branch offices connect to the corporate network from campus, branch, or private home offices and access the resources distributed across locations. The federation eliminates redundant log ins and host checks and provides seamless access to protected resources. The federation uses IF-MAP protocol to share information about user sessions between ICS and IPS over the distributed network.

For more information about IF-MAP, see http://www.trustedcomputinggroup.org/wp-content/uploads/TNC_IFMAP_v1_1_r5.pdf

IF-MAP Federation Use Cases

This section describes the various IF-MAP use cases. Using IF-MAP federation the users can seamlessly access with a single log in to corporate resources protected by the firewall. It provisions seamless access between the user sessions of ICS and IPS.

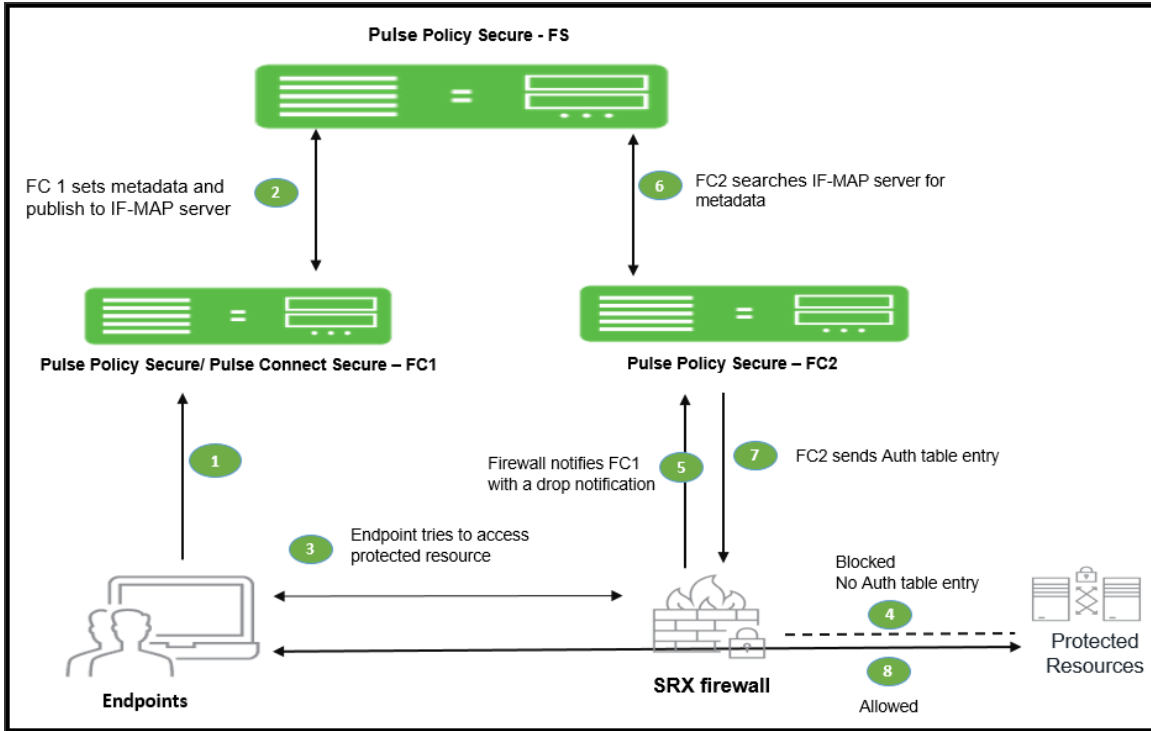
Access Control in the Federated Enterprise

In a federated enterprise, a user can log in to a IPS or ICS device for authentication or remote access and access the resource protected by the firewall connected to another IPS. The session information is shared across IPS or ICS device using IF-MAP protocol through IF-MAP server.

The federation requires dynamic auth table provisioning on the SRX firewall and allows access to the protected resource based on the resource access policies that are configured on IPS.

The access solution serves the following objectives:

- Ensures that the employees can access the corporate network and can access resources and data in both local and remote locations without having to specify their authentication credentials at each security policy enforcement point.
- Enhances security by enforcing role or policy based access control.



The session federation work flow is described below:

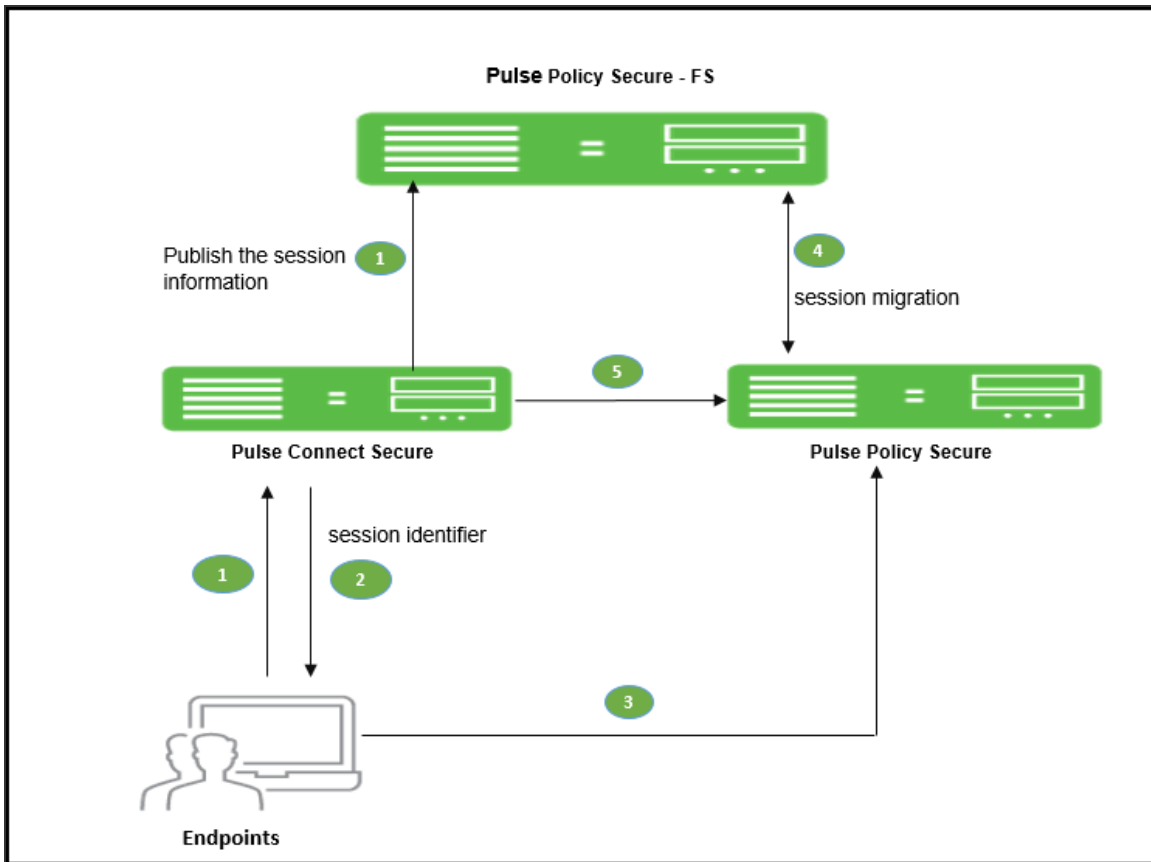
1. The user connects to network and authenticates with IPS/ICS (FC1).
2. Authentication information such as IP address, MAC address, username, and roles are published to the IF-MAP server.
3. The user tries to access protected resource from the branch office.
4. The firewall blocks the access.
5. The firewall requests IPS (FC2) for session details such as user roles. IPS device subscribes to session information and other endpoint data based on the originating IP address.
6. The federation server sends the search result based on the search request from IPS (FC2).
7. IPS (FC2) send roles and policy information to the firewall.
8. The firewall allows or denies traffic based on the resource access policies received from FC2.

Session Migration across ICS and IPS using IF-MAP

IF-MAP federation allows seamless access to the users connected through remote access and on premise network without re-authenticating. For example, a user can connect from home through ICS and then arrive at work and connect through IPS without logging in again. The session migration also enables users to access different resources within the network that are protected by internal devices without repeatedly providing credentials.

When a session is migrated, realm role-mapping rules determine user access capabilities. You can import user attributes when a session is migrated, or you can configure a dedicated directory server to look up attributes for migrated user sessions. To ensure that session migration retains user sessions, configure a limited access remediation role that does not require a Host Checker policy. This role is necessary because the Host Checker timeout can be exceeded if an endpoint is in hibernation or asleep. With the new remediation role, the user's session is maintained. The session migration works only with same authentication group.

If additional Host Checker policies are configured on a role or realm to which a migrated session applies, the policies are performed before allowing the user to access the role or realm. Administrators of different Pulse servers should ensure that Host Checker policies are appropriately configured for endpoint compatibility.



The session migration workflow is as follows:

1. User connects to ICS and the information is published to the federation server, which includes session identifier.
2. The session identifier information is also communicated to Pulse client.
3. When user connect to IPS in the same authentication group after arriving at office network using Pulse client.
4. The Pulse client sends session identifier to IPS.
5. IPS appliance uses the session identifier to look up the session information in the IF-MAP server and request to migrate the session from ICS to IPS.
6. IPS create a local session for the endpoint.

To permit session migration for users with the Pulse client, perform the following tasks:

1. Configure location awareness rules within a client connection set to specify locations included in the scope of session migration for users. For example, configure location awareness rules for a corporate IPS server connection and a ICS server connection.
2. Configure an IF-MAP federated network, with the applicable Pulse servers as IF-MAP Federation clients of the same IF-MAP Federation server.
3. Ensure that user entries are configured on the authentication server for each gateway.
4. Ensure that user roles are configured for all users on each gateway.
5. Define a remediation role with no Host Checker policies to allow user sessions to be maintained when an endpoint is sleeping or hibernating.
6. Configure role-mapping rules that permit users to access resources on each gateway.
7. Enable and configure session migration from the User Realms page of the admin console.
8. Distribute the Pulse client to users.

Configuring Session Migration for Pulse Client

Ensure that all of the IPS and ICS servers for which you want to enable session migration are IF-MAP

Federation clients of the same IF-MAP Federation server. Additionally, make sure that each gateway is configured according to the procedures outlined in this section.

To configure session migration:

1. In the admin console, select **Users > User Realms**.
2. Select an existing realm, or create a new realm.
3. On the General page, select the **Session Migration** check box. Additional options appear.
4. In the Authentication Group box, enter a string that is common to all of the gateways
5. that provision session migration for users. The authentication group is used as an
6. identifier.
7. Select for either the **Use Attributes from IF-MAP** option button or the **Lookup Attributes using Directory Server** option.



Select Lookup Attributes using Directory Server only if you are using an LDAP server. Attributes are served faster with an LDAP server.

User Realms > Cert Auth > General

General

General | Authentication Policy | Role Mapping

* Name:

Description:

When editing, start on the Role Mapping page

▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication:

User Directory/Attribute:

Accounting:

Device Attributes:

▼ Additional Authentication Server

Enable additional authentication server

▼ Dynamic policy evaluation

Enable dynamic policy evaluation

▼ Session Migration

Session Migration

Session migration allows Pulse Secure clients to maintain a session across different Pulse Policy Secure and Pulse Connect Secure devices without requiring reauthentication.

Authentication Group: A string that determines which sessions may be migrated or shared

Inbound Sessions:

Use Attributes from IF-MAP

Lookup Attributes using Directory Server

▼ Other Settings

Authentication Policy: Certificate restrictions

Role Mapping: Password restrictions

No Rules

* indicates required field

Authentication Server Support

The behavior of session migration depends to some extent on the authentication server on the inbound side.

The following list provides a summary of authentication server support:

- Local authentication server-Migration succeeds if the username is valid on the local authentication server.
- LDAP server-Migration succeeds if the LDAP authentication server can resolve the username to a distinguished name (DN).
- NIS server-Migration succeeds if the NIS authentication server can find the username on the NIS server.
- ACE server-Migration always succeeds.
- RADIUS server-Migration always succeeds. If you select Lookup Attributes using Directory Server, no attributes are present in the user context data.
- Active Directory-Migration always succeeds. The Lookup Attributes using Directory Server option may not work, depending on your configuration.
- Certificate-Migration succeeds if the certificate is valid.
- SAML-Migration always succeeds because Identity provider is external server.
- Anonymous-No support for migrating sessions because sessions are not authenticated.
- Siteminder-No support for migrating sessions because Siteminder SSO is used instead.

IF-MAP Configuration

The IF-MAP configuration involves configuring the IPS device as an IF-MAP client or an IF-MAP server. You can configure the ICS device as an IF-MAP client for an IF-MAP server. A device configured as an IF-MAP server is automatically a client of itself. An IF-MAP server can function as a fully functional IPS device and any endpoint sessions with an IP address created on an IF-MAP server are automatically published to that IF-MAP server.

Configuring IF-MAP Server

An IF-MAP server is a repository for IF-MAP clients, which is used for publishing information regarding an activity on the network. To deploy IPS as an IF-MAP server, you must configure IPS as an IF-MAP server and then add IPS/ICS as IF-MAP clients. A IPS device can be deployed as a dedicated IF-MAP server for better scale and performance. If you opt for this configuration it consumes most of the virtual memory available on appliance, which results in performance degradation of other IPS services.



Currently, only Active/Passive cluster mode for IF-MAP server is supported.

To configure IF-MAP server on the IPS:

1. Select **System > IF-MAP Federation > Overview**.

2. Select **IF-MAP Server** option
(Optional) Select **Enhance IF-MAP server storage** for using the appliance as a dedicated federation server for high scalability.
3. Click **Save Changes**.

Adding IF-MAP Clients

The IF-MAP client must be added for subscribing the session information on an IF-MAP server. You configure an entry for each IF-MAP client on the IF-MAP server.

To add IF-MAP client:

1. Select **System > IF-MAP Federation > This Server > Clients**.
2. Click **New IF-MAP Client**.

3. Under IF-MAP Client,
 - Enter name and optionally a description for client.
 - Enter one or more IP addresses of the client.
 - If the client is connected to multiple data links on the same network or different network, then list all of its physical network interfaces.
 - If the client is a IPS cluster, then list the internal and external network interfaces of all nodes. You must enter all of the IP addresses for all of the interfaces because equipment failures may cause traffic between the IF-MAP client and the IF-MAP server to be re-routed through a different network interface. Listing all of the IP addresses maximizes the probability that IF-MAP Federation still works in the event of a failure.
4. Under Authentication, select the Client Authentication Method: **Basic** or **Certificate**.
 - If you select **Basic**, enter a Username and Password. The same information should be added to the IF-MAP server.
 - If you select **Certificate**, choose which Certificate Authority (CA) to use to verify the certificate for this client. Optionally, specify certificate attributes or restrictions to require values for certain client certificate attributes.
5. Click **Save Changes**.

Configuring IF-MAP Client

The IF-MAP client publishes the basic session information, which includes IP address, usernames, and roles. The IF-MAP server stores the information as metadata. Other IF-MAP clients in the network can poll the server for metadata information when the endpoint tries to access the protected resource. A ICS or IPS device can be deployed as an IF-MAP client. The IPS device connected to firewall is always added as an IF-MAP client. You must import the trusted root CA certificate of the federation sever device certificate issuing cert store in to IF-MAP client for secure connection. You can trust the certificate issued by CA of server's device certificate by importing the root certificate of the issuing authority.

To configure the IF-MAP client:

1. Select **System > IF-MAP Federation > Overview**.
2. Select **IF-MAP Client**.

IF-MAP > Overview

Overview

Overview This Client

An IF-MAP federation simplifies the work of end users by letting network devices share information about user sessions. For example, if a user connects to the network using Connect Secure, they can automatically gain access (if authorized) to protected resources that are behind Infranet Enforcer firewalls, without having to log in again.

Choose whether this Pulse Policy Secure runs an IF-MAP Server, an IF-MAP client, or no IF-MAP

IF-MAP Server
 IF-MAP Client
 No IF-MAP

An IF-MAP Server is automatically an IF-MAP client of itself

Server URL

* Server URL: Example: https://ic/dana-ws/soap/dsifmap

Authentication

Basic
 Certificate
 Certificate

* Username:

* Password:

Save Changes Cancel

3. Enter **IF-MAP server IP address** or complete IF-MAP server URL. For IF-MAP server in cluster mode use the virtual IP address (VIP).

4. Select the Client Authentication Method: **Basic** or **Certificate**.
 - Select **Basic authentication**, and enter the **username** and **password**. This is the same as the information that you entered on the IF-MAP server.
 - Select Certificate, select the Device Certificate to use.
5. Ensure that the certificate of the CA that signed the IF-MAP server certificate is added from the **System > Configuration > Certificates > Trusted Server CA page**.
6. Ensure that the hostname in the IF-MAP URL on the client machine matches the hostname of the server certificate on the IF-MAP server and that the CA that signed the server certificate is configured as trusted server CA on the IF-MAP client.
7. Click **Save Changes**.

The status light on the server's IF-MAP Federation > This Server > Clients page is green when the client and server are successfully connected.

Configuring IF MAP Policies

The IF-MAP policies allows you to perform the data synchronization operations between the IF-MAP server and IF-MAP clients.

Session Export Policies

The session export policy specifies how to transform Pulse Client session data into IF-MAP standard data. It allows IF-MAP clients to translate outgoing session information into IF-MAP data and incoming IF-MAP data into session information. These translations enable sessions to be shared between ICS and IPS even if the devices sharing sessions have different role configurations.

To configure a session export policy:

1. Select **System > IF-MAP Federation > Session-Export Policies**.
2. Click **New** to create a new policy.

The screenshot shows the configuration interface for a new policy. At the top, the 'Policy Type' is set to 'Session Export'. Below this are input fields for 'Policy Name' and 'Policy Description'. The main section is titled 'Apply policy for these roles:' and contains two columns: 'Available Roles' and 'Selected Roles'. The 'Available Roles' list includes Engg, Guest, Guest Admin, OnboardRole, remed, Remediation, and Users. There are 'Add ->' and 'Remove' buttons between the columns. Below the role selection is a section for 'Policy Actions' with a dropdown arrow. The 'Set IF-MAP Capabilities' option is checked, and the 'Copy matching roles' radio button is selected. A note states 'IF-MAP capabilities are similar to Pulse Policy Secure and Pulse Connect Secure roles'. There is an empty text area for specifying capabilities. At the bottom, there is a 'View Advanced Actions' section with a checkbox for 'Stop processing policies when this policy matches.' and 'Save Changes' and 'Cancel' buttons.

3. Enter a policy name and, optionally, a description.
4. Select role and add if the policy needs to be applied to selected roles only, otherwise by default is to apply policy for all roles.
5. Under Policy Actions, select **Set IF-MAP Capabilities** and select the applicable option:
 - **Copy Matching Roles**-Copies all of the user roles that match the roles specified in the Roles section of this policy into the IF-MAP capabilities data.
 - **Copy all Roles**-Copies all of the roles from the user session to the IF-MAP capabilities data.
 - **Set capabilities specified below**-Enter capabilities, one per line.

To configure advanced options:

1. Select the **View Advanced Actions** link to display additional options.
2. Select **Set IF-MAP Identity** and configure identity settings:
 - **Identity Type** -Select an element used to specify identity. Options include aik-name, distinguished-name, dns-name, email-address, kerberos-principal, trusted-platform-model, username, sip-uri, tel-uri, and other. For example, for a regular employee named Bob Smith you can select username as the Identity Type and enter the Identity as username bsmith.
 - **Identity**-Identity is normally specified as <NAME>, which assigns the user's log in name. Any combination of literal text and context variables may be specified. If you select other for Identity Type, enter a unique Identity Type in the text box.
 - **Administrative Domain**-This optional information is applied to identity and MAC address data. One example for using this field is in a large network environment with several domains in which a username could be duplicated. By supplying the domain, you ensure that the correct user is identified.
 - **Other**-This field is provided for advanced use cases when none of the predefined options are applicable.
3. Select **Set IF-MAP Roles** and select the applicable option:
 - **Copy Matching Roles**-Copies all of the user roles that match the roles specified in the Roles section of this policy into the IF-MAP capabilities data.
 - **Copy all Roles**-Copies all of the roles from the user session to the IF-MAP capabilities data.
 - **Set capabilities specified below**-Enter capabilities, one per line.
4. Select **Set IF-MAP Device Attributes**. Device attributes represent a passed Host Checker policy on PIPSPS or ICS. Select the applicable option:
 - **Copy Host Checker policy names**-The name of each Host Checker policy that passed for the session is copied to a device attribute.
 - **Set Device Attributes**-Enter device attributes, one per line.
5. Select **Stop processing policies when this policy matches** to specify that when this policy is matched, no more Session-Export policies should be applied.

6. Select **Save Changes** or continue to configure advanced actions.

Session Import Policies

The session import policies specify how the device derives a username and a set of roles based on IF-MAP data that it receives from the IF-MAP server. The import policies are similar to role mapping rules on a realm. You must be precise when you configure Import policies, otherwise roles cannot be assigned properly.

To configure session-import policies:

1. Select **System > IF-MAP > Session-Import Policies**.
2. Click **New** to create a new policy.

IF-MAP > This Client > IF-MAP session import policies > Session-Import Policy

Session-Import Policy

Policy Type: Session Import

Policy Name:

Policy Description:

▼ Conditions when Policy Applies

Match IF-MAP Capabilities Makes this policy apply only when a federation-wide session has particular capabilities. IF-MAP capabilities are similar to Pulse Policy Secure roles

• View Advanced Conditions

▼ Assign these roles

Use these roles

Copy IF-MAP Capabilities

All capabilities

Specified capabilities

All capabilities other than those specified below

• View Advanced Assignment Option

Stop processing policies when this policy matches.

3. Type a policy name and, optionally, a description.
4. Under Conditions when Policy Applies, select **Match IF-MAP Capabilities**. You can use the wildcard characters * and % to match IF-MAP capabilities.

5. Enter IF-MAP capabilities exactly as they appear in the corresponding session-export policy. For example, if you assigned the value "engineering" to an IF-MAP capability in the session-export policy, enter "engineering" here.
6. Under "Assign these roles," select **Use these roles** and select the roles for which the policy applies.
7. Alternatively, select **Copy IF-MAP Capabilities**. If you select this check box, IF-MAP session capabilities on the IF-MAP server are converted to IPS roles with the same name. You can use this option if IPS roles and IF-MAP capabilities have the same name. This option is typically not required for IPS deployments.
8. Select **Stop processing policies** when this policy matches to specify that when this policy is matched, no more Session-Export policies should be applied.
9. Select **Save Changes**, or continue to configure Advanced Conditions.
You can configure advanced options that would further require that Identity, Role, or Device Attributes in the IF-MAP data for a session must match before applying the role matching. The advanced options are not required for most IPS IF-MAP deployments.

To configure advanced options:

1. Select the **View Advanced Conditions** link to additional options.
2. Select one or more of the following check boxes to specify which IF-MAP criteria to use for assigning roles:
You can use the wildcard characters * and % to match IF-MAP capabilities.
 - If you select **Match IF-MAP Identity**, complete the following settings:
 - **Identity Type**-Select an element used to specify identity. Options include aik-name, distinguished-name, dns-name, email-address, kerberos-principal, trusted-platform-model, username, sip-uri, tel-uri, and other. For example, for a regular employee named Bob Smith you can select username as the Identity Type and enter the Identity as username bsmith.
 - **Identity**-Identity is normally specified as <NAME>, which assigns the user's log in name. Any combination of literal text and context variables may be specified. If you select other for Identity Type, enter a unique Identity Type in the text box.
 - **Administrative Domain**-This optional information is applied to identity and MAC address data. One example for using this field is in a large network environment with several domains in which a username could be duplicated. By supplying the domain, you ensure that the correct user is identified.
 - **Other**-This field is provided for advanced use cases when none of the predefined options are applicable.
 - **Match IF-MAP Roles**-Enter individual roles in the provided text box.
 - **Match IF-MAP Device Attributes**-Enter individual device attributes in the provided text box.
3. Click **Save Changes**.

Active Federated Session Details

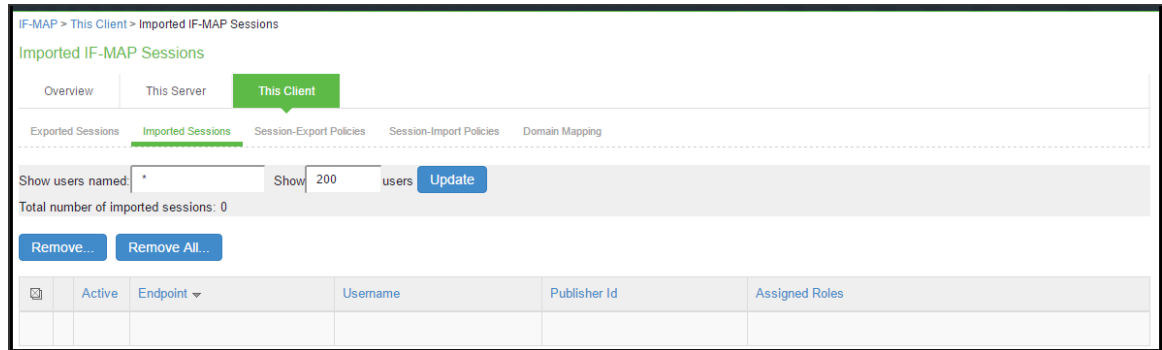
The federated session details of all the active users can be viewed on both the IF-MAP client and the IF-MAP server.

Imported Session Details

The session details from IPS, which are provisioned to SRX firewall can be viewed on an IF-MAP client.

To view, remove, or remove all the current sessions on an IF-MAP client:

1. Select **System > IF-MAP Federation > This Client**.
2. Select **Imported Sessions**.



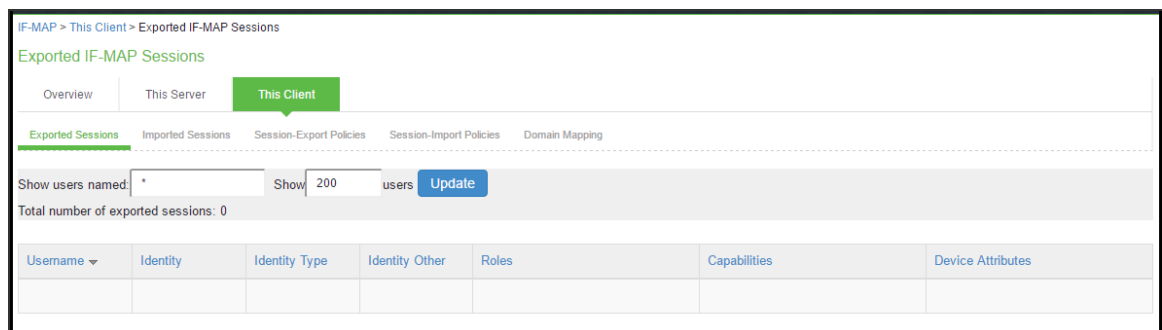
3. Select **Remove** or **Remove All** to remove the imported federated session(s) from the device and the associated authentication table entries.

Exported Session Details

On an IF-MAP client, you can view all sessions from other IPS appliances that are currently published to firewall.

To view the exported sessions:

1. Select **System > IF-MAP Federation > This Client**.
2. Select **Exported Sessions**.

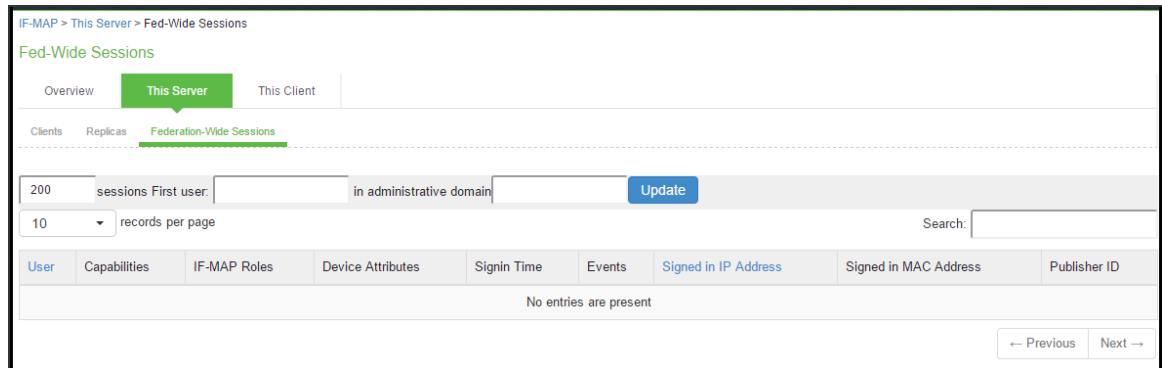


Federated Session Details

The federated sessions published to the server can be viewed on an IF-MAP server. The IF-MAP server purges sessions about 3.5 minutes after the client disconnects. The exceptions are if the server is currently involved in a purge or immediately after the server starts. It takes several minutes to scan the database before a purge can begin.

To view details about users and their sessions, and perform detailed searches:

1. Select **System > IF-MAP Federation > This Server > Federation-Wide Sessions**.



2. Enter users and administrative domain and click **Update** to search for specific session information.
3. Sort users on the page by selecting User or Signed in IP Address.



- The maximum number of session entries displayed in the Federation-Wide Sessions table or returned by the query to the table is 5,000 entries.
- You can also view IF-MAP session-export details by selecting the IF-MAP check box at Troubleshooting > User Sessions > Policy Tracing in the admin console.

Troubleshooting

The following diagnostic tools on IPS can assist you in troubleshooting the federated network:

- **IF-MAP Client User Messages**-On the IF-MAP client, logs information that is published to and removed from the IF-MAP server. Enable IF-MAP Client User Messages by selecting Log/Monitoring > User Access > Settings on the IPS IF-MAP client.

- **IF-MAP Server Trace**-On the IF-MAP server, logs the XML for all IF-MAP requests and responses. Enable the IF-MAP Server Trace by selecting Log/Monitoring > Events > Settings on the IF-MAP server. IF-MAP Server Trace should only be enabled for troubleshooting purposes, because running this diagnostic incurs a large performance impact.
- **Debuglog** - Select Troubleshooting > Monitoring > Debug Log, use event code dsfederate for debugging logs.

The admin logs help to debug the configuration issues. Ensure that the server root CA certificate is imported to avoid configuration issues.

If the IF-MAP server loses the connectivity due to hard failures and reconnects back within 3 minutes, then the access to protected resources is not affected. If the connection is lost for more than 3 minutes the access to protected resource is suspended till the users tries to access the resource.

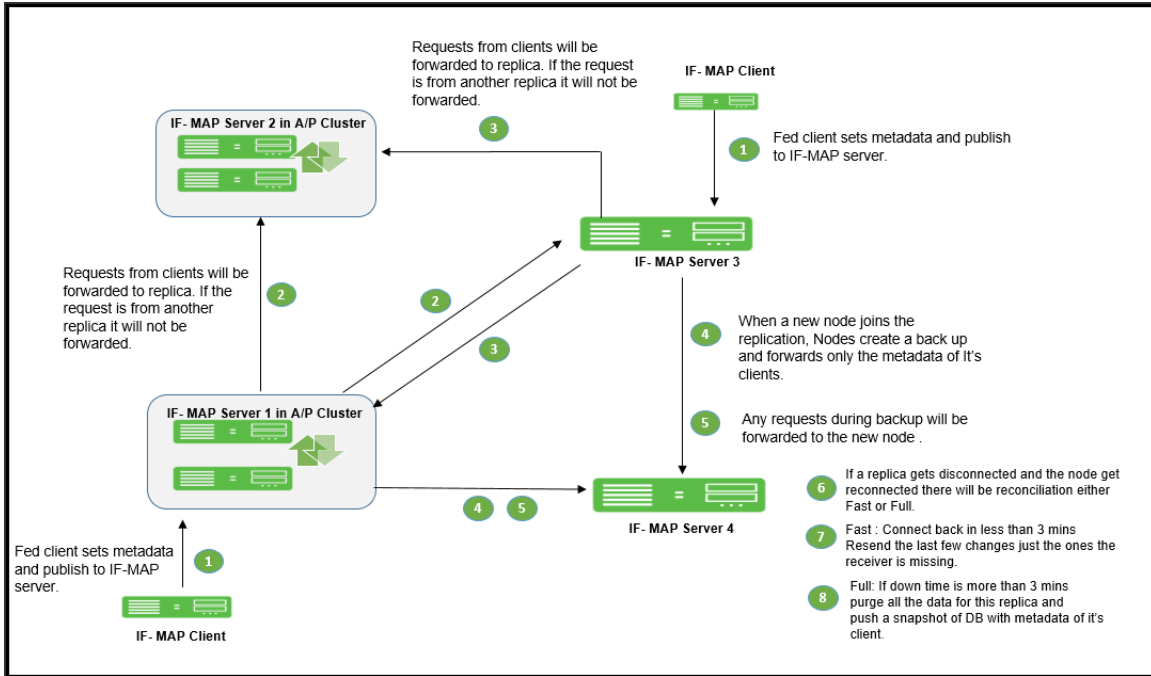
Appendix

Clustering in a Federated Deployment

You can deploy clustered IPS appliance as IF-MAP servers or IF-MAP clients. You can configure IF-MAP servers in an Active Passive cluster. IF-MAP clients must be configured with the cluster's virtual IP (VIP) and must communicate with only the active node.

The session changes in federation cluster networks are propagated rapidly. The clients can access resources without experiencing delays, and there is no single point of failure. If any single device fails, the passive node recovers in seconds. You can configure IF-MAP client in Active/Active or Active/Passive cluster.

You can also use clustered IPS appliances as server replicas. The following figure illustrates a complex network of clustered and standalone IPS appliance.

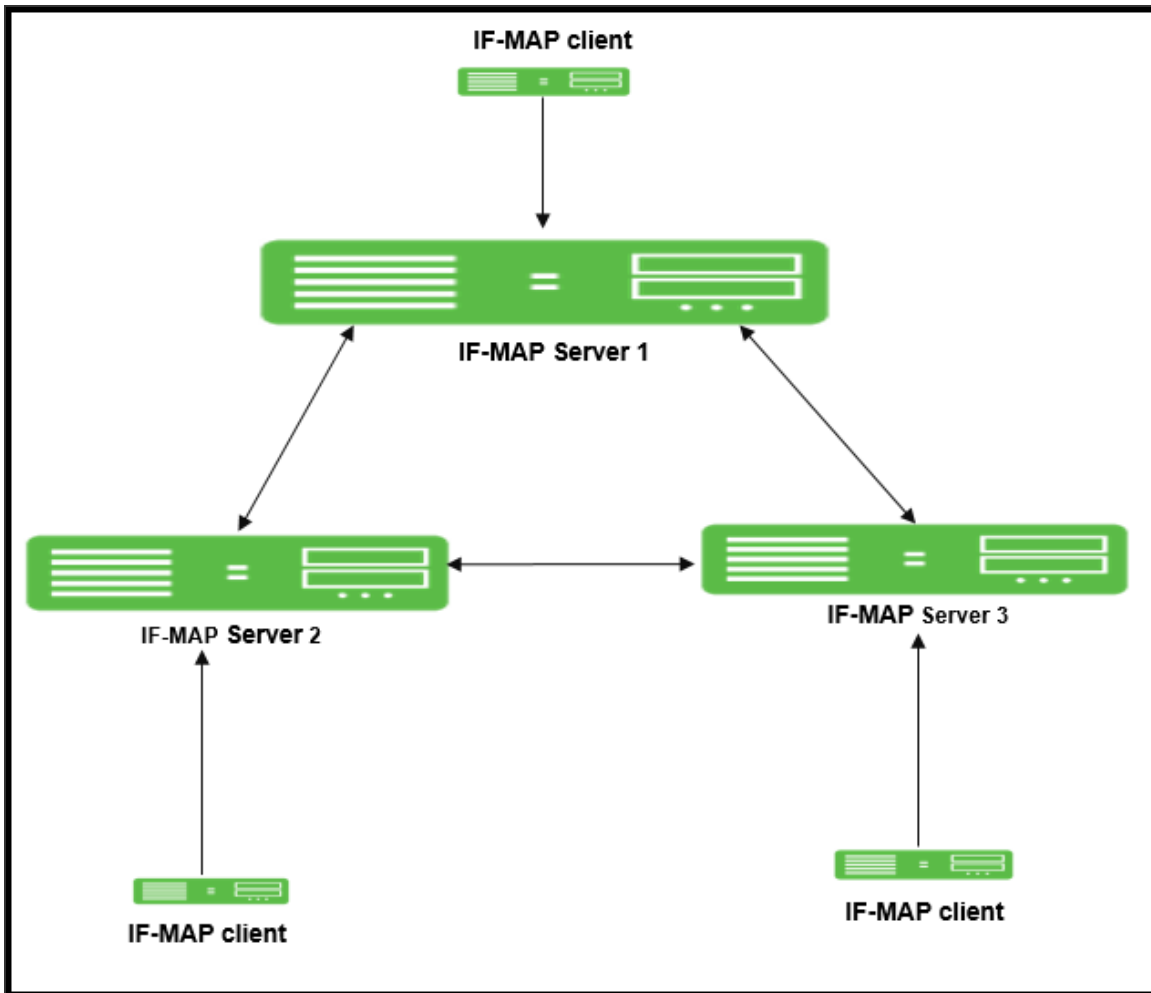


Replica IF-MAP Server

The IF-MAP server has the capability to replicate all of its IF-MAP data to other IF-MAP servers. For example, if you have a network in Boston and a network in London, you can run IF-MAP servers in both places and configure the IF-MAP servers in both locations to replicate data to one another. An endpoint that accesses IPS or ICS can access protected resources behind any of the IPS devices connected to local or replica IF-MAP server.

Each replica IF-MAP server communicates in a bidirectional way with all the connected IF-MAP server replicas. The data on each IF-MAP server is available on every server and enhances the system performance. A 3-way replica in mesh topology in which all the servers are connected to each other is supported.

The following figure depicts one possible deployment replica scenario.



Bandwidth issues determine the effectiveness of the entire IF-MAP Federation's operation. A key to timeliness is that IF-MAP servers should generally be placed geographically close to IF-MAP clients to ensure the most efficient operation. Replicas in an IF-MAP federated network allow user session data to be shared over greater distance. For example, the user in Boston can connect with servers in London through the replicated IF-MAP server in London.

To configure IF-MAP server replicas to communicate:

1. Select **System > IF-MAP Federation > This Server**.
2. Click the **Replicas** tab and then select **New IF-MAP replica to configure Replica settings**.

The screenshot shows the 'New IF-MAP Replicas' configuration page. The breadcrumb trail is 'IF-MAP > This Server > Replicas > New IF-MAP Replicas'. The page title is 'New IF-MAP Replicas'. There are two main sections: 'IF-MAP replica' and 'Authentication'. The 'IF-MAP replica' section contains four input fields: 'Name' (with a tooltip 'Label to reference this IF-MAP replica'), 'Description', 'Hostname' (with a tooltip 'Hostname for outbound connections to the replica. Must match the replica's device certificate'), and 'IP addresses' (with a tooltip 'All possible source IP addresses for inbound connections from the replica'). The 'Authentication' section has two radio buttons: 'Basic' and 'Certificate'. A 'Save Changes' button is located at the bottom of the form.

3. Type a Name for the replica IF-MAP server.
4. (Optional) Enter a Description for the replica or replica network.
5. For **Hostname**, enter the hostname that exactly matches the replica's device certificate. This is used when this IF-MAP server initiates a connection to the replica. Use the fully qualified domain name (FQDN) of the replica's internal or external interface. For a cluster, use the FQDN of the internal or external VIP.
6. After **IP addresses**, provide one or more IP addresses from which the replica can initiate connections to this server. If the replica is standalone, for survivability list both the internal and external network interfaces. If the replica is a cluster, for survivability list the internal and external network interfaces of both cluster nodes.
7. Select the Authentication method: **Basic** or **Certificate**.
8. For **Basic**, enter a username and password.
9. For **Certificate**, select the CA that issued the IF-MAP replica's certificate. Enter restrictions, one per line. If any restrictions match, (for example CN=ic.example.com), the certificate is accepted.
10. Click **Save Changes** to create the connection for the replica.

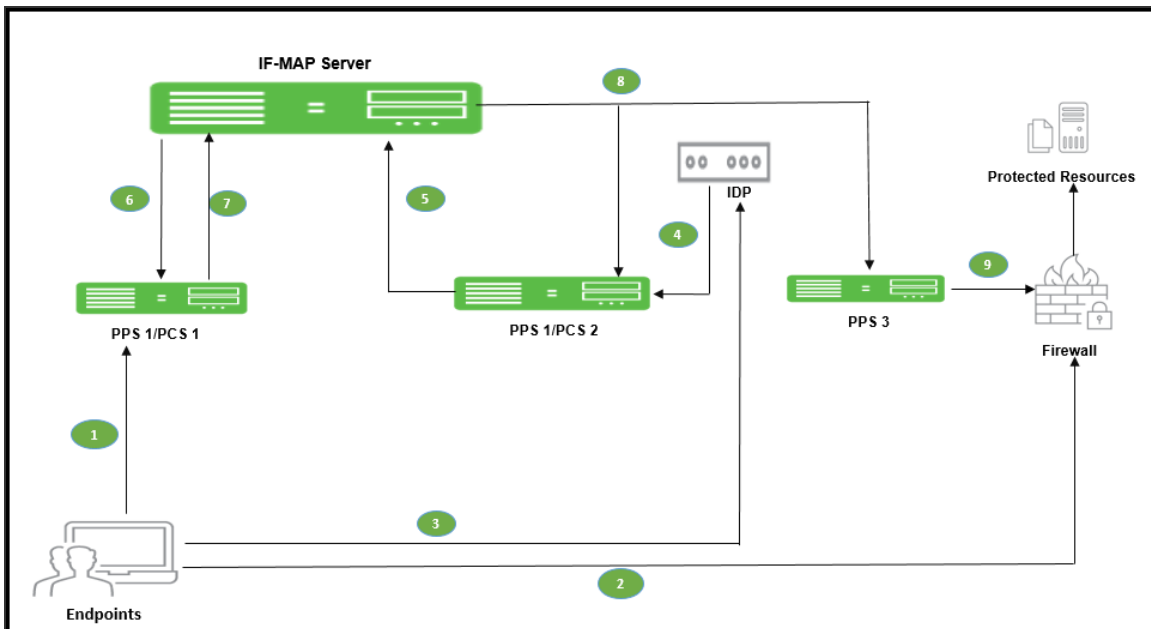
Coordinated Threat Control in a Federated Environment

You can use Juniper Networks IDP Series Intrusion Detection and Prevention Appliance with Federation to detect attacks from within the network. Any endpoint that is on any connected IPS device or ICS can be monitored for suspicious activity. IF-MAP clients can work together to provide coordinated threat control across all attached enforcement points.

Endpoints that access ICS can be monitored by standalone IDP. Endpoints that access IPS device can be monitored by either standalone IDP, Integrated Security Gateway Intrusion Detection and Prevention ISG-IDP, or SRX Series Services Gateway IDP.

The IDP device reports attacks to the IPS or ICS to which it is connected. The IPS or ICS configured as an IF-MAP client reports the user's activity to the IF-MAP server using IF-MAP. The IF-MAP server notifies the authenticating IPS or ICS about the attack, and the authenticating device applies its IDP sensor policies. If new roles or restrictions are imposed on the endpoint based on policies configured on the device, the IPS or ICS publishes the new session information for the endpoint to the IF-MAP server.

When any other IPS or ICS polls the IF-MAP server, the newly published session information for the user determines the protected resources that the user can access. The following figure shows a deployment with IDP.



The following steps summarize the interaction with IDP in an IF-MAP federated network.

1. The endpoint successfully accesses IPS or ICS 1 and publishes session data to the IF-MAP server through Session-Export policies.
2. The endpoint attempts to access protected resources behind the SRX firewall, which is connected to IPS 3. IPS 3 uses IF-MAP to query the IF-MAP server for session information about the endpoint. After receiving session information, IPS 3 uses Session-Import policies to determine roles and then provisions an auth table entry on the SRX firewall. IPS 3 subscribes to updates about the endpoint's session data.
3. After the endpoint is successfully connected to resources behind the SRX firewall, IDP detects an attack originating from the endpoint.
4. IDP notifies IPS 2 of the attack. (If IDP is standalone IDP, IPS 2 could also be an ICS. If IDP is an SRX firewall with the ISG-IDP security module, IPS 2 cannot be a ICS, because the ICS does not communicate with the SRX firewall.)
5. IPS 2 updates the endpoint session data on the IF-MAP server with information about the attack.
6. The IF-MAP server notifies IPS or ICS 1 (the original authenticating device) about the attack. The authenticating IPS or ICS is responsible for consuming the attack.
7. The authenticating IPS or ICS applies its sensor policies to the endpoint and updates the endpoint's session according to actions specified in the sensor policies. For example, the endpoint must be assigned a more restrictive role. The IPS or ICS publishes the new session information to the IF-MAP server, and the new information replaces the old data.
8. The IF-MAP server notifies any IPS that subscribe to updates about the endpoint. This includes IPS 3, which is connected to the SRX firewall.
9. IPS 3 applies Session-Import policies to the new session data for the endpoint and pushes the resulting roles to the SRX firewall.
10. If the new set of roles denies access to the protected resources, access is denied.

Performance and Scalability

The IF-MAP server is supported on both hardware and virtual platforms.

The scalability of the IF-MAP server depends on:

- Type of platform- Hardware or VM image.
- If the IF-MAP server is used as a dedicated IF-MAP server and the virtual memory available. You must configure IPS as dedicated only when you want it to be fully used as an IF-MAP server and not for other processes such as authentication.
- Number of roles and attributes.
- For example, PSA 7000 has no impact of dedicated IF-MAP server setting option due to kernel memory limit of process. With single role for session, scale limit is up to 300K fed-wide sessions.
- PSA5000/SM360/PSA3000, the scale limit is 150K fed-wide session on dedicated IF-MAP appliance.
- For virtual platform (VM image), scalability is limited and based on the size of virtual memory.

The performance on IF-MAP server is described below:

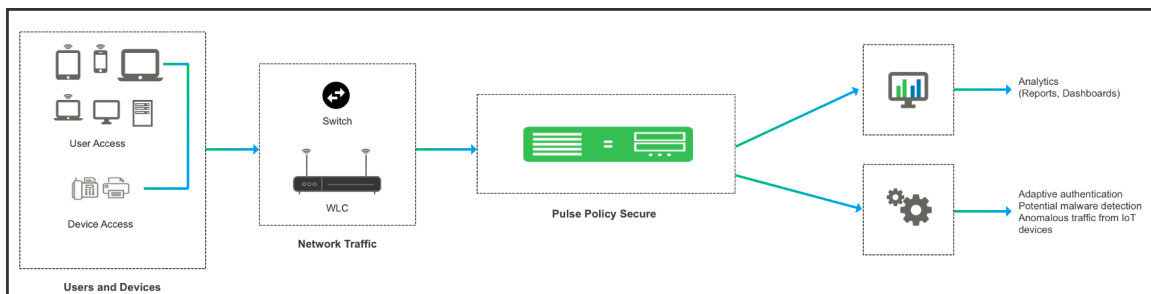
- The IF-MAP server supports 24 export/import requests together per second.
- The time interval required to access the resource protected by the firewall after the user log in is 20 seconds.
- Latency and bandwidth between IF-MAP replicas affect the amount of time taken to replicate large amounts of data during heavy IF-MAP server utilization.
- The IF-MAP federation replica is supported over transatlantic link, however we might face issues due to WAN connection and latency between the devices.
- For clustering or replication, there is no impact on the scalability.

Behavioral Analytics

Overview

Enterprises deal with constant and ever-increasing magnitude of threat vectors, which includes Data Loss Prevention (DLP), malware and Domain Generation Algorithms (DGA) attacks. With changing business requirements and new types of threats, Administrators must understand how users and devices are accessing company's data and services to ensure that the access control policies are up to date. Even after successful authentication the user's activity should be monitored fully to ensure device compliance. Policy rules for protecting resources need to be configured and should be resistant to new attacks. Policy rules are configured manually, and the process is not scalable with new attacks. Hence, it is very important for Administrators to have insights into any anomalous behavior and act accordingly.

Behavioral Analytics feature analyzes user's action along with other context data to derive conclusions about any anomalous activities. It provides information/visibility based on real time user or device context thus helping in advanced attack detection and helps in proactive policy-based enforcement.



The Behavioral Analytics feature analyzes user or device behavior using the following methods:

- **Adaptive Authentication-** User/device is prompted for second level of authentication based on the threat profile determined for the corresponding user/device.

Below are some of the scenarios where second level of authentication is required:

- **User authenticating from new device:** This is detected by using the device MAC address.
- **User authenticating from new location:** Location details are obtained by using the subnet and location configurations.

- Anomalous Traffic from IoT devices: The unmanaged and IoT devices are profiled during the learning period configured in IPS. Any Anomalous traffic from these devices is detected as an anomaly based on the known profile of the device. IPS uses both Netflow and SPAN configuration on switches for detecting anomalous traffic from IoT devices.
- Potential Malware Detection: Malware on client devices have become more intelligent and in generating domain names by using dynamic generation algorithms. Hence, using rule-based policies might not detect these anomalies. IPS uses SPAN data collection method for monitoring DNS traffic and detects these potential malware on the endpoint.

Adaptive authentication user flow

- Users connect to IPS.
- IPS performs the primary authentication.
- IPS checks for any anomalies.
- IPS prompts for secondary authentication for the first login or if the user location changes.
- User enters the credentials required for secondary authentication.
- IPS performs the secondary authentication and allows/rejects access to the user/device.

Anomalous traffic from IoT devices user flow:

1. User/Device establishes a connection with IPS.
2. Switch and DNS Server forwards the network traffic of the device to IPS.
3. IPS analyzes the network traffic and takes the action based on the detected anomaly.

Potential malware detection user flow:

1. User/Device establishes a connection with IPS.
2. DNS server forwards all the domain resolutions to IPS.
3. IPS analyzes the DNS traffic and detects potential malware on the endpoint.

Licensing

- Adaptive Authentication feature is part of the IPS license.
- Anomalous Traffic detection from IoT devices and Potential Malware detection feature requires Behavioral Analytics license to be installed on IPS.

Benefits

- Monitors the traffic from user/devices and helps in determining the possible anomalous activities such as:
 - User is authenticating from a new device/new location.
 - Device traffic is different from previous instances.
 - Potential malware on the endpoint.
- Data collected as part of Behavioral Analytics is stored so that it can be used later for determining the anomalies.

Configurations

Pre-Requisites

IPS determines the network anomalies based on the NetFlow and Switch Port Analyzer (SPAN) configurations on the switch.

- Enable NetFlow (v5 or v9) and port mirroring/SPAN on switches. For sample configurations, see [Appendix](#).
- NetFlow traffic is currently qualified only with Cisco switches.

Summary of Configuration

1. Administrator enables the Behavioral Analytics feature and configures IPS based on the use case (Adaptive Authentication, anomaly traffic detection, potential malware detection). The Admin configures the list of switches in the network from where the network traffic can be received/forwarded to analytics engine on IPS.

2. Administrator configures the role mapping rules to consume these flags and control the access to the corresponding users and devices.
3. Administrator enables the secondary authentication for the users in case they are tagged with anomalies activities to ensure additional level of authentication for security purpose.
4. View the Dashboard and Reports for any detected anomalies.
5. From the Reports page, Administrator has options to clear the detected anomalies, export the available anomaly data to a CSV file.



- Behavioral Analytics configuration is synched across the nodes in the cluster (including config-only clusters). However, data collected and analyzed is synched across the nodes but not in case of config-only clusters.
- RSPAN is the recommended configuration for cluster deployments especially for the Active/Passive cluster for seamless VIP failover.
- Adaptive authentication is not supported for 802.1.x connections using native supplicant.

Configuring IPS for enabling Behavioral Analytics

For the fresh Installation of IPS, UEBA package will not be available by default for anomaly detection. Admin must add the UEBA package. In case of upgrade of IPS (R7 or earlier to R8 or later), the previous UEBA package is retained. You may download latest UEBA package from Ivanti Secure Support Site (<https://my.pulsesecure.net>).

UEBA Package

To upload the UEBA package:

1. Log in to Ivanti Support Site, <https://my.pulsesecure.net>.
2. Select Ivanti Policy Secure as product and navigate to the "Ivanti Behavioral Analytics Database" section. Download the package, "ps-pcs-pps-behavioral-analytics-v1.0.x.pkg".
3. From the Admin Console, select **System > Behavioral Analytics**.
4. Navigate to Browse and select the UEBA package.
5. Click **Upload & Activate**.
6. Click **Save Changes**.

Configuring IPS for Adaptive Authentication

To enable adaptive authentication:

1. Select **System > Behavioral Analytics > Configuration**.
2. Under Configurations, select **Enable Behavioral Analytics**.
3. For enabling Adaptive Authentication, select **Enable data collection** during authentication of devices and users.
 - For location-based anomaly detection, select **Enable subnet** based location anomaly detection.
4. Enter the Subnet details. For example, 10.11.1.2/24.
5. Enter the location name.
6. Type the location to search and press Enter.
7. Click **Add** to add the location.

Enable Behavioral Analytics

Enable data collection during authentication of devices and users

Enable subnet based location anomaly detection

Subnet	Location Name	Location	
<input type="text"/>	<input type="text"/>	<input type="text" value="Search for Location..."/> © OpenStreetMap contributors	<input type="button" value="Add"/>
<input type="radio"/>	BANGALORE	Bengaluru, Bangalore Urban, Karnataka, India	
<input type="radio"/>	MUMBAI	Mumbai, Mumbai City, Maharashtra, India	
<input type="radio"/>	HYDERABAD	Hyderabad, Telangana, India	

Example subnet: 10.11.1.2/24 or f5a6:f136:c4c7:5554::/64

8. Select **User > User Realms > General**.

9. Under Additional Authentication Server, **Enable Additional Authentication Server**.
 - Select **Enable Adaptive authentication**.
 - Under Authentication #2, select the desired secondary authentication server from the drop-down list.

Additional Authentication Server

Enable additional authentication server

You can specify an additional authentication server. The additional credentials can be specified by the user on the sign-in page (the labels for these inputs are specified by the sign-in

Enable adaptive authentication

Note: Adaptive authentication is supported by leveraging the behavioral analytics. Enable behavioral analytics on 'System->Behavioral Analytics->Configuration' for supporting this. Ac server above.

Authentication #2:

Username is:

- specified by user on sign-in page
- predefined as:

Password is:

- specified by user on sign-in page
- predefined as: Mask static password

End session if authentication against this server fails

10. Click **Save Changes**.

Configuring IPS to detect Anomaly Traffic from IoT devices

As a pre-requisite Profiler should have been configured for detecting the anomaly traffic from IoT devices. For more information, see *Profiler Deployment Guide*.

To determine anomaly traffic from IoT devices:

1. Select **System > Behavioral Analytics > Configuration**.
2. Under Configurations, select **Enable Behavioral Analytics**.

3. Select **Enable Network Traffic** from switches.
 - Configure the list of switches in the network from where the required data can be received/forwarded to analytics engine on IPS.
 - **Add the switches** manually by adding (Switch IP address/mac address) or add the existing switches under Add Switch from list table. Select **Dynamically add switches from RADIUS and SNMP** clients to automatically add switches from RADIUS and SNMP clients.
4. Select **Enable Data Collection through SPAN from switch to enable SPAN configuration** for determining unknown domain anomaly for unmanaged devices.
 - Select the network interface (External port/Internal port).
 - (Optional) Enter the IP address of the DNS server and click Add. DNS requests from these servers will not be considered for anomaly detection.

- Enter the learning duration in days (7-30 days). Learning duration is learning period for unmanaged devices to build the device profile.

Enable Network Traffic Monitoring from switches
Note: This is used for detection of Anomalous traffic from IoT devices

▼ **Add switches manually**
 Add switches manually for monitoring netflow traffic.

Delete ▲ ▼

Switch IP	
<input style="width: 95%;" type="text"/>	<input type="button" value="Add"/>

Example: 10.1.1.2 or 10.1.1.20/28 or fda6:f136:c4c7:5554::/64 or fda6:f136:c4c7:5554::

▼ **Add switches from list**
 Add existing switches from the list which are configured as RADIUS or SNMP clients for monitoring netflow traffic.

Switch	IP	Type	<input type="checkbox"/> Select all
Cisco	10.1.1.6	Radius	<input checked="" type="checkbox"/>

Dynamically add switches from RADIUS and SNMP Clients
Note: Selecting this option will automatically add switches from RADIUS and SNMP clients for monitoring network traffic.

Enable data collection through SPAN from switch
Note: This is used for Malware detection and Anomalous traffic from IoT devices

Select Network Interface: External port Note: The selected interface cannot be used for any other traffic.

DNS Servers	
<input style="width: 95%;" type="text"/>	<input type="button" value="Add"/>
<input checked="" type="radio"/> 10.30.74.14	

Note: DNS requests from DNS servers will not be considered for domain anomaly detection. Example: 10.1.1.2

White listed domains	
<input style="width: 95%;" type="text"/>	<input type="button" value="Add"/>

Note: Whitelisted domains will not be considered as DGA attack domain. Ex: abc.com

Learning duration: days Number of days for which the system collects data for computing the baseline for an endpoint. The value should be between 7 to 30 days.

- Click **Save Changes**.

7. Configure the role mapping rules for user realm and/or MAC authentication realm.
 - Create new role mapping rule, select **Anomaly attribute under Rule** based on and click **Update**.
 - Enter the rule name.
 - Under Rule: If device has any of the following anomaly types:
 - **Any of the anomalies found**- Select this option to detect the device with any anomaly type.
 - **Select from list of anomalies**- Select this option to configure the specific anomaly type from the available list. To detect anomaly traffic from IoT devices configure **Unknown server/Unknown domain** as anomaly from the list of **Available Anomaly Types**.
 - Select **Stop processing more rules** option to stop evaluating role mapping rules if the user meets the conditions specified for this rule. Ensure that the rule is at the top of the list.
8. Configure the required roles and click **Save Changes**.

Configuring IPS to detect Potential Malware

IPS relies on DNS traffic collected through SPAN to determine the potential malware on the endpoint.

To configure IPS for detecting potential malware:

1. Select **System > Behavioral Analytics > Configuration**.
2. Under Configurations, select **Enable Behavioral Analytics**.
3. Select **Enable Data Collection through SPAN** from switch to enable SPAN configuration for determining DGA based potential malware attacks. This anomaly detection mechanism is supported for both managed and unmanaged/IoT devices.
 - Select the network interface (External port/Internal port).
 - (Optional) Enter the IP address of the DNS server and click **Add**. DNS requests from these servers will not be considered for anomaly detection.
 - (Optional) Enter the white listed domains to exempt the domains from anomaly detection.

Enable data collection through SPAN from switch
Note: This is used for Malware detection and Anomalous traffic from IoT devices

Select Network Interface: **External port** Note: The selected interface cannot be used for any other traffic.

DNS Servers	
<input type="text"/>	Add
<input type="text"/>	

Note: DNS requests from DNS servers will not be considered for domain anomaly detection. Example: 10.1.1.2

White listed domains	
<input type="text"/>	Add
<input type="text"/>	

Note: Whitelisted domains will not be considered as DGA attack domain. Ex: abc.com

Learning duration: days Number of days for which the system collects data for computing the baseline for an endpoint. The value should be between 7 to 30 days.

Save Changes

4. Configure the role mapping rules for user realm and/or MAC authentication realm.
 - Create new role mapping rule, select **Anomaly attribute** under **Rule based on** and click **Update**.
 - Enter the rule name.
 - Under Rule: If device has any of the following anomaly types:
 - **Any of the anomalies found**- Select this option to detect the device with any anomaly type.
 - **Select from list of anomalies**- Select this option to configure the specific anomaly type from the available list. To detect potential malware from IoT devices configure **DGA** as anomaly from the list of **Available Anomaly Types**.
 - Select **Stop processing more rules** option to stop evaluating role mapping rules if the user meets the conditions specified for this rule. Ensure that the rule is at the top of the list.



The Administrator can also create Anomaly rules based on Custom Expressions.

5. Click **Save Changes**.

Dashboard and Reports

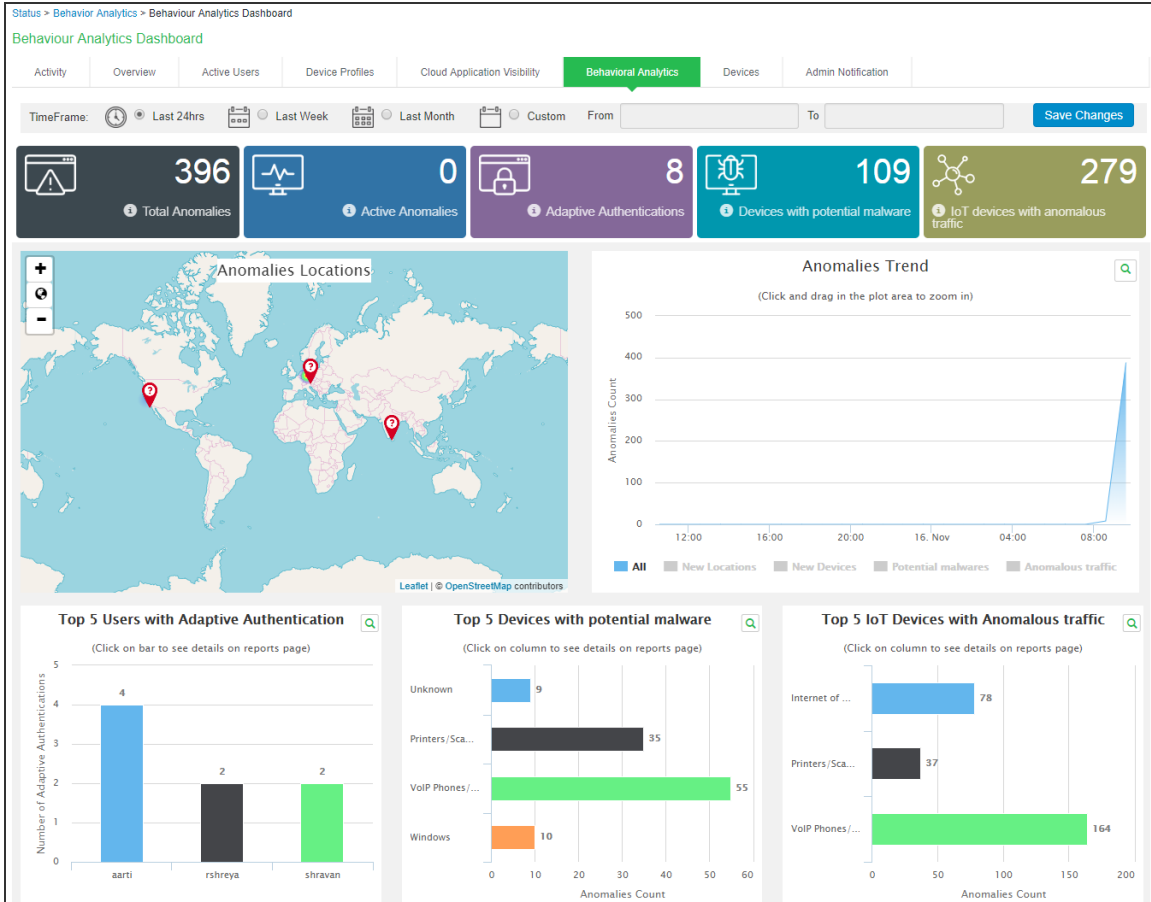
The Behavioral Analytics dashboard provides visibility to many anomalies in the network. It provides visibility of any known, active anomalies, devices with potential malware, IoT devices with anomalous traffic, anomalies location, trend and so on.

To view the Behavioral analytics dashboard:

1. Select **System > Status > Behavioral Analytics**.
2. Select the desired timeframe from available options.
3. Click **Save Changes**.

You can also view the drill down reports such as:

- Top 5 Users with Adaptive Authentication
- Top 5 Devices with Potential Malware
- Top 5 Devices with Anomalous Traffic



To view the Behavioural Analytics reports, select **System > Reports > Behavioral Analytics**.

Reports - Behavioral Analytics User Report

Behavioral Analytics | Infected Devices


Showing 1 to 3 of 3 entries | 10 records per page

User Name	Anomalies Count	Recent Anomaly Detection Time	Recent IP Address	Recent MAC Address	Recent Location	Actions
[Redacted]	3	Fri, 02 Nov 2018 11:18:14	[Redacted]	[Redacted]	MUMBAI	Clear
[Redacted]	5	Fri, 02 Nov 2018 11:16:16	[Redacted]	[Redacted]	MUMBAI	Clear
[Redacted]	2	Fri, 02 Nov 2018 10:52:05	[Redacted]	[Redacted]	MUMBAI	Clear

Advanced Filters: From [] First Previous 1 Next Last

User Name: **rbhays**

Location History



Leaflet | © OpenStreetMap contributors

User History

2 records per page Search:

Location	Number of Logins	Last Login Time	MAC Address	IP Address
MUMBAI	2	Fri, 02 Nov 2018 11:23:09	[REDACTED]	[REDACTED]
HYDERABAD	1	Fri, 02 Nov 2018 10:53:23	08-00-80-00-00-1E	[REDACTED]

Reports > Behavioral Analytics > Behavioral Analytics Network Report

Reports

Behavioral Analytics Network Report

User Summary | Single User Activities | Device Summary | Single Device Activities | Device Discovery | Application Discovery | Authentication | Compliance

Behavioral Analytics | Infected Devices

User | **Network**

Clear All

Showing 1 to 3 of 3 entries 10 records per page All Search Actions

	MAC Address	Device Category	Anomalies Count	Recent Anomaly Detection Time	Recent IP Address	Recent Locations	Actions
Last 24hrs	[REDACTED]	Internet of Things (IoT)	22	Fri, 02 Nov 2018 11:36:21	1 [REDACTED]	MUMBAI	Clear
Last Week	[REDACTED]	Projectors	50	Fri, 02 Nov 2018 11:34:58	1 [REDACTED]	BANGALORE	Clear
Last Month	[REDACTED]	Windows	7	Fri, 02 Nov 2018 11:31:16	1 [REDACTED]	HYDERABAD	Clear

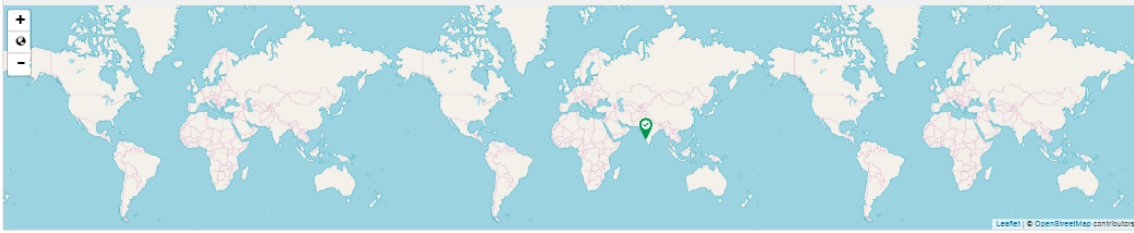
Advanced Filters

From

First Previous 1 Next Last

Mac Address: 00-50-56-bf-3c-49

Location



Device History

2 records per page Search: [] 2 records per page Search: []

Domains: No data available in table

Destination Servers: No data available in table

Anomalies

2 records per page Search: []

Last Detected Time	Category	IP Address	Anomaly Type	Value	Count
Fri, 02 Nov 2018 11:39:21	Internet of Things (IoT)	[REDACTED]	Unknown domain	dns.mafncsl.com	2
Fri, 02 Nov 2018 11:34:37	Internet of Things (IoT)	[REDACTED]	Unknown domain	safebrowsing.googleapis.com	1

Previous 1 2 3 4 5 Next

Troubleshooting

The event and debug logs can be used for troubleshooting:

The Event logs are generated for the device related anomalies:

- Anomalous traffic from IoT devices
- Potential malware

You can use the User Access and Admin Logs in case of any issues. The user access logs are generated whenever there are any user related anomalies such as user logging from new location/device/new user. The Admin Logs are generated whenever there is a change with Behavioral Analytics options and if there are any changes with respect to application policies.

You can also use **Maintenance > Troubleshooting > Monitoring > Debug Log** for debugging issues. Enable debug log with events *ueba*.

Appendix

SPAN

Switched Port Analyzer (SPAN) allows you to send a copy of traffic passing through ports to another port on the switch. SPAN is important to mirror received or transmitted (or both) traffic on one or more source ports to a destination port for analysis.

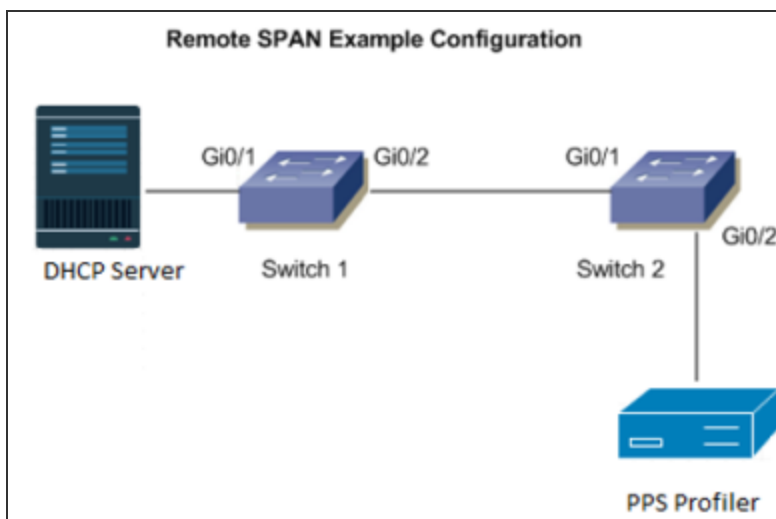
SPAN is mirroring ports in the same switch, RSPAN (Remote SPAN) is mirroring ports in one switch to a port in different switch.

This example describes how to configure RSPAN on Cisco Catalyst switches (Cisco 2960).

RSPAN

A sample topology to monitor traffic on port Gi0/1 in Switch1 using a IPS Profiler connected to port Gi0/2 in Switch2 is shown below.

Create a VLAN that will be used as an RSPAN-VLAN on both switches. In this example vlan ID 999 is used as the RSPAN-VLAN. Allow the RSPAN-VLAN on the trunk port between Switch1 and Switch2.



Switch1 (Source switch)

```
Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#vlan 999
Switch1(config-vlan)#name RSPAN-Vlan
Switch1(config-vlan)#remote-span
```

```
Switch1(config-vlan)#exit
Switch1(config)#monitor session 1 source interface Gi0/1
Switch1(config)#monitor session 1 destination remote vlan 999
Switch1(config)#end
```

Allow VLAN ID 999 on the trunk port Gi0/2

```
Switch1#sh run int g0/2
Building configuration...
Current configuration : 175 bytes
!
interface GigabitEthernet0/2
description To-Switch2-port-Gi0/1
switchport trunk allowed vlan 74,999
switchport mode trunk
end
```

Switch2 (destination switch)

```
Switch2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#vlan 999
Switch2(config-vlan)#name RSPAN-Vlan
Switch2(config-vlan)#remote-span
Switch2(config-vlan)#exit
Switch2(config)#monitor session 1 source remote vlan 999
Switch2(config)#end
```

Allow vlan id 999 on the trunk port Gi0/1

```
Switch2#sh run int g0/1
Building configuration...
Current configuration : 175 bytes
!
interface GigabitEthernet0/1
description To-Switch1-port-Gi0/2
switchport trunk allowed vlan 10,20,30,999,60
switchport mode trunk
end
```

Allow VLAN id 999 on trunk port Gi0/2.

```
Switch1#sh run int g0/2
Building configuration...
```

```

Current configuration : 175 bytes
!
interface GigabitEthernet0/2
description To-Switch2-port-Gi0/2
switchport trunk allowed vlan 60,999
switchport mode trunk
end

```

NetFlow

NetFlow is a network protocol developed by Cisco for collecting IP traffic information and monitoring network traffic. Using a NetFlow collector and analyzer, you can see where network traffic is coming from and going to and how much traffic is being generated.

NetFlow V5 or V9 has to be configured on Cisco switch.

Commands on Cisco Switch

```

ueba-switch(config)#flow exporter UEBA
ueba-switch(config-flow-exporter)# destination <IPS IP>
ueba-switch(config-flow-exporter)#transport udp 2055
ueba-switch(config-flow-exporter)#export-protocol netflow-v9 (or netflow-v5)

```



Cisco 3850 Catalyst switches support only v9 whereas Cisco 2960 supports both v5 and v9

```

ueba-switch(config)#flow record UEBA
ueba-switch(config-flow-record)# match ipv4 protocol
ueba-switch(config-flow-record)#match ipv4 source address
ueba-switch(config-flow-record)#match ipv4 destination address
ueba-switch(config-flow-record)# match transport source-port
ueba-switch(config-flow-record)#match transport destination-port
ueba-switch(config-flow-record)#match interface input
ueba-switch(config-flow-record)#collect interface output
ueba-switch(config)#flow monitor UEBA
ueba-switch(config-flow-monitor)#exporter UEBA
ueba-switch(config-flow-monitor)#cache timeout active 60
ueba-switch(config-flow-monitor)#record UEBA
ueba-switch(config)#interface GigabitEthernet1/0/3 --- (interface to which client
endpoint is connected)
ueba-switch(config-if)#ip flow monitor UEBA input

```

IoT Access

IoT Policy Provisioning

This chapter provides an overview of IoT device enforcement using SRX/PAN firewall.

Overview

As we increasingly connect devices to the Internet, new opportunities to exploit potential security vulnerabilities grow. Any unknown devices including IoT devices could serve as entry points for cyberattack by allowing malicious individuals to re-program a device or cause it to malfunction. The IoT devices are being added to corporate networks with or without the knowledge of IT administrator and they may communicate using the corporate IP network. These devices may have limited security controls leaving them open to be used as an attack vector. To improve security posture of IoT devices in corporate network, visibility and Role Based Access Control play a key role. Hence, it's extremely important to detect and classify what's there on the network.

IPS along with Profiler enables you to secure and manage access to IoT devices. It allows you to configure IoT Access Policy based on discovered or profiled device category. It also allows you to dynamically configure resource access policies for newly discovered devices and map user's role-based access to specific category and manufacturer or profile group of IoT devices.

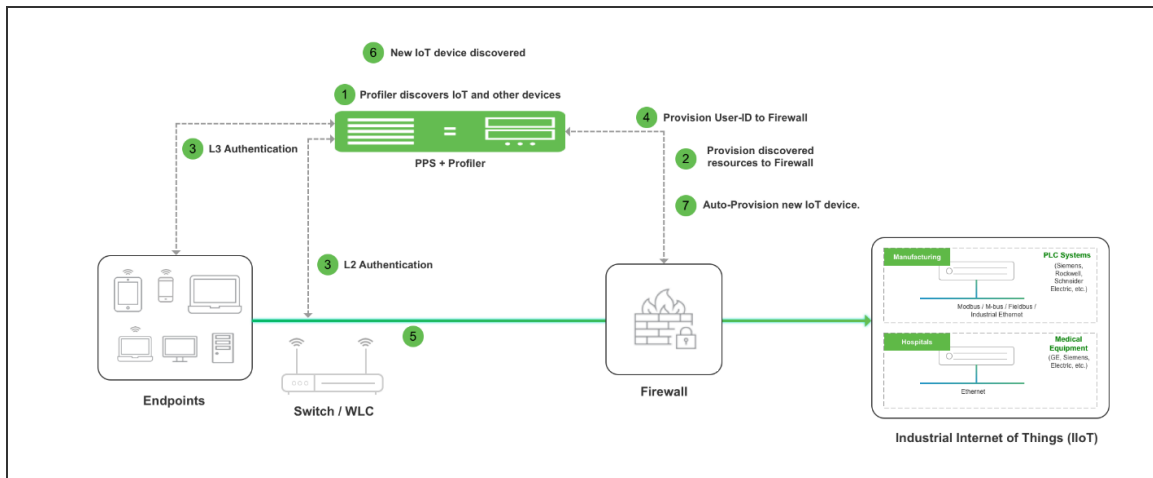
Benefits

The IoT Policy Provisioning Page enables you to quickly configure IoT policy provisioning and provides the following benefits:

- Discover and profile IoT devices using Profiler. Profiler enables you to continuously monitor the network and discover new devices such as security cameras, sensors, Industrial IoT devices (IIoT), medical sensors, and so on.
- IPS provides IoT access control using the IoT Access Policies, which are created automatically based on profiled or newly discovered device information from Profiler.
- Reduce IoT/IIoT machine downtime by allowing authorised users to get a role-based access to specific IoT/IIoT device for troubleshooting/maintenance.
- Automatic access control for the newly discovered IoT devices.

Deployments

The below network diagram depicts how IPS, Profiler, and SRX/PAN Firewall can be deployed to protect access to IoT devices. For example, the manufacturing domain consists of different IoT devices to monitor and control the manufacturing process. The industrial IoT devices are separated and controlled behind the firewall. IPS enables you to define IoT Access Policy using the Profiler attributes (category and manufacturer or profile group) and provides secure and seamless access to IoT devices for authorized users.



The workflow is described below:

1. A local Profiler configured on IPS discovers devices including IoT devices connected to corporate network.
2. IPS leverages the list of IoT devices discovered using Profiler and based on device category and manufacturer or profile group and it enforces or controls the access to IoT devices protected by the firewall.
3. User authenticates to IPS and endpoint compliance is evaluated. The user session is created on IPS and appropriate role is assigned based on the compliance check and user ID.
4. User Identity details (AuthTable) are provisioned to firewall.
5. User tries to access IoT devices protected by firewall. Authorised users (based on roles) are allowed to access IoT devices. Access to IoT devices by unauthorised users is blocked.
6. A new IoT device is added to the corporate network and same is discovered by Profiler.

- IoT Access Policy for the newly discovered IoT device is automatically pushed to SRX/PAN firewall.



Only Local Profiler is currently supported.

The Administrator can group the discovered devices based on any Profiler attributes. For more information see, [Configuring Profiler Groups](#).

Configuring IoT Policy Provisioning

This section covers the procedure for configuring IoT Policy Provisioning on IPS.

Pre-Requisite

IoT Policy Provisioning requires Profiler feature. You must install the Profiler license on IPS to enable it.

Summary of Configuration

A high-level overview of the configuration steps needed to set up IoT Policy Provisioning is shown below.

Step 1: Configure Profiler

Step 2: Configure SRX/PAN Enforcer

Step 3: [Configuring IoT Access Policy](#)

Step 3.1: [Viewing Devices in Enforcer Policy Report](#)

Step 3.2: [Configuring IoT Access Policy using Juniper SRX Firewall](#)

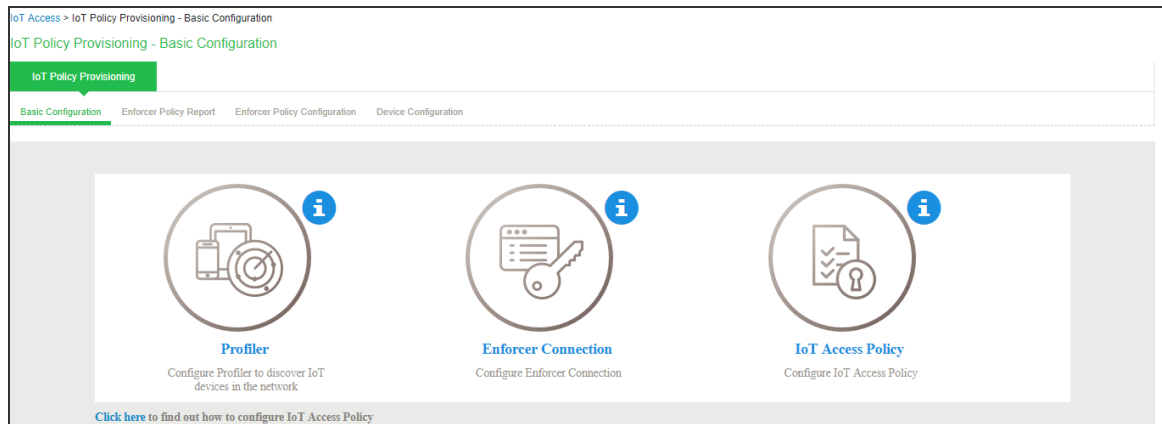
Step 4: Configuring Additional Device Category/Profile Groups

Basic Configurations

- The basic configuration page enables you to configure Profiler to discover IoT devices in the network,
- Enforcer to push the user identity information to IPS, and IoT Access Policy for IoT devices.

To launch the configuration page:

1. Select **Endpoint Policy > IoT Access > IoT Policy Provisioning**.
2. Click **Basic Configuration**.



If IPS is already configured with Profiler and Enforcer. The configurations will be reused.

3. Configure the Profiler used to discover the IoT devices in the network. Click **Profiler** and configure the local Profiler. See *Profiler Deployment Guide* for complete configuration.
 - The icons in the configuration page indicate the status of configuration.
 - Green Tick mark refers that this section is configured correctly.
 - If the configuration section is in grey color, it indicates that the section is not configured.
 - Information icon refers that this section has to be configured.

Auth Servers > Profiler > Settings

Settings

Settings | Troubleshooting | Browse Fingerprints

* Name: Label to reference this server.

▼ **Fingerprint Database file**

No file chosen [Browse](#) [Upload and Save](#)

Last uploaded version: 32 | Last imported on: Thu Jun 14 12:14:00 2018

▼ **General Settings**

* Poll Interval: Minutes: Specify the interval to check Switch for connected endpoints. Default=60 minimum=5 To discover devices, configure one or more switches under [Network Infrastructure Device](#)

* DHCP Sniffing mode: Select an option based on your DHCP forward mode.

▼ **Device Sponsoring**

Select device categories that will trigger an email to the admin for approval. Create a role-mapping rule based on "status" attribute to assign the device to the respective role before and after approval.
 Note: Devices can be approved or unapproved from the [Device Discovery Report](#).

BSD Datacenter appliance Gaming Consoles Home Audio/Video Equipment Internet of Things (IoT)
 Linux Macintosh Medical Device Monitoring Devices Network Boot Agents
 Other OS Physical Security Point of Sale devices Printers/Scanners Projectors
 Routers and APs Smartphones/PDAs/Tablets Storage Devices Switches Thin Clients
 Video Conferencing VoIP Phones/Adapters Windows

Approver's email address to send notifications. Multiple addresses can be separated by a semicolon(,).

SMTP server configuration is required for sending emails. Currently SMTP server is not enabled. [Click here to configure.](#)

* URL for Device Discovery Report.
 It will appear in the notification email as a link for quick access to the devices that need approval. Profiler hostname or IP address is needed to complete the URL.

https:///dana-admin/reporting/report_device_discovery.cgi

▼ **Endpoints to scan using NMAP/WMI/SSH**

Once devices are discovered using DHCP, SNMP or other mechanisms, more granular profiling is done only for those devices using NMAP, WMI and SSH active scan. Use the following subnet configuration to either allow, or disallow, such scans. Maximum 100 subnets.

[Delete](#) [↑](#) [↓](#)

Subnet	Include/Exclude	Collector	
<input type="text"/>	<input checked="" type="radio"/> Include <input type="radio"/> Exclude	<input checked="" type="checkbox"/> NMAP <input type="checkbox"/> WMI <input type="checkbox"/> SSH	Add

Subnets should be in valid CIDR format or individual IP or IP Range.
 Example Subnets:
 Valid CIDR Format:
 192.168.1.0/24
 10.200.0.0/16
 IP or IP-Range:
 10.10.10.10
 10.10.10.10-100
 10.10.1.1-10.10.5.200

▼ **WMI Profiling**

Configure WMI credentials. Use Active Directory server credentials.

*User: User or domain/user or user@domain.com for endpoints.

*Password: [Test Credentials](#)

Endpoint ip or hostname on which credentials can be tested

▼ **SSH Profiling**

Authentication Method:

*User: RSA key owner

*Private key: RSA private key

passphrase: Passphrase used for generating key

[Test Credentials](#)

Endpoint ip or hostname on which credentials can be tested

▼ **MDM Server**

MDM server: Specify an MDM server that the Profiler may contact to collect additional endpoint attributes

[Save Changes](#) [Reset](#)

- Configure the SRX/PAN Enforcer. Click **Enforcer Connection** and add **SRX/PAN** as a **New Enforcer**.

Infranet Enforcer > Connection > SRX

SRX

Connection

▼ Infranet Enforcer

Platform: JUNOS SRX Platform of this Infranet Enforcer.

* Name: SRX Label to reference this Infranet Enforcer.

* Password: Connection password.

* Serial number(s): CF1314AK0016 One per line.

Location Group: - No 802.1X - To manage groups, see the [Location Group](#)

▼ Coordinated Threat Control

Note that not all enforcer versions and platforms have an IDP module.

Use IDP Module as Sensor

Save Changes

* indicates required field

Infranet Enforcer > Connection > pan

pan

Connection

▼ Infranet Enforcer

Platform: Palo Alto Networks Firewall Platform of this Infranet Enforcer.

* Name: pan Label to reference this Infranet Enforcer.

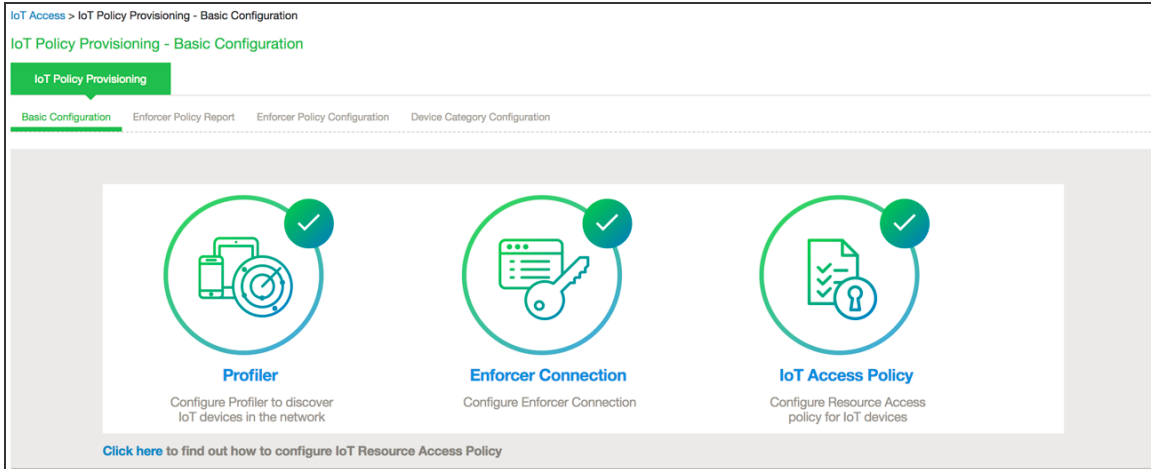
* IP Address: IP Address of this Infranet Enforcer

* API Key: Get API Key Auto-completed when you retrieve the API Key

Server Certificate Validation: Enable this option to verify the firewall's certificate

Save Changes

Once the configuration is complete and successful, the Administrator can see the configuration status as shown in figure.



Configuring IoT Access Policy

Viewing Devices in Enforcer Policy Report

This page provides details of discovered and connected IoT device's and firewall policies applied for IoT devices. You can view details such as total number of IoT devices, number of IoT devices enforced, number of IoT devices not enforced, and IoT device manufacturers.

To view the enforcer policy report:

1. Select **Endpoint Policy > IoT Access > IoT Policy Provisioning**.
2. Click **Enforcer Policy Report**.

The screenshot shows the 'IoT Policy Provisioning - Enforcer Policy Report' page. It features a summary dashboard with five cards showing statistics:

- 213** Total Number of IoT Devices
- 38** IoT Devices - Policy Enforced
- 175** IoT Devices - Policy Not Enforced
- 9** IoT Device Manufacturers
- 1** IoT Device Groups

 Below the dashboard is a table with columns for Category, IP, Hostname, Manufacturer, Profile Group, Enforcers, Roles, Action, and Policy. The table contains several rows of data, including entries for 'Internet of Things (IoT)' and 'Network Boot Agents'.

Category	IP	Hostname	Manufacturer	Profile Group	Enforcers	Roles	Action	Policy
Internet of Things (IoT)	10.255.0.100	host127	Apple, Inc.	IoT	SRX (SRX)	All roles	Allow	Policy
Internet of Things (IoT)		host127	Apple, Inc.	IoT	PAN1 (PAN)	Users	Allow	Network Boot Agents
Network Boot Agents			Super Micro Computer, Inc.	Network Boot Agents	PAN1 (PAN)	Users	Allow	Network Boot Agents
Network Boot Agents			VMware, Inc.	Network Boot Agents	PAN1 (PAN)	Users	Allow	Network Boot Agents
Network Boot Agents	10.255.0.100		Super Micro Computer, Inc.	Network Boot Agents	PAN1 (PAN)	Users	Allow	Network Boot Agents

Configuring IoT Access Policy using Juniper SRX Firewall

The IoT access policy specifies which users are allowed or denied access to a set of protected resources. You can specify which users you want to allow or deny by choosing the roles for each IoT Access Policy. The IoT Access Policy page enables you to configure the policy based on device details using Profiler device attributes, such as device category and manufacturer or profile group.

When the network Administrator selects category and manufacturer or profile group information under device details the IP addresses of the corresponding discovered devices get automatically updated under Resources. Hence the Administrator can seamlessly create IoT Access Policy of profiled devices based on device category, device manufacturer attributes, or Profiler group. If the Administrator wants to have granular control over the IoT devices, further control can be achieved by providing specific port and protocol. The specified port and protocol configuration is applied to all the discovered devices of the selected category and manufacturers.

To configure IoT access policy:

1. Select **Endpoint Policy > IoT Access > IoT Policy Provisioning > Enforcer Policy Configuration**.
2. Click **New Policy**.
3. Enter the Policy name.
4. Enter a description.
5. Under Infranet Enforcer, select the Platform as **Junos SRX**.

6. Under **Device Details**, specify whether the policy should be applied based on device category and manufacturer or Profile group.

- Category and manufacturer
 - Specify the category from the drop-down list. The values in the drop-down list is populated based on the Device category configuration (IoT Access > IoT Policy Provisioning - Device Configuration).
 - Select the Device manufacturer from the Available Device Manufacturers.
 - Specify the protocol (TCP/UDP/ICMP) and Port/Range to be applied to the discovered devices.
- Profile Group
 - Configure the Profiler Group (IoT Access > IoT Policy Provisioning - Device Configuration). To configure Profiler Groups, [Configuring Profiler Groups](#).
 - Select the Profile Group from the Available Profile Groups.
 - Specify the protocol (TCP/UDP/ICMP) and Port/Range to be applied to the discovered devices.



Port ranges must be configured in dash-separated, comma-delimited, ascending, and non-overlapping order. Multiple port ranges must be separated by a comma. For example, the following examples show the delimiters that are used to enter port ranges:(80, 443, 1-1024, 1-100, 500-600).

The Port/Range entered will be applied to all the discovered devices. If you want to enter different port values, you can edit the port value under Resources table.

- Select **Auto-Update Newly Discovered** Devices to automatically add IoT Access Policy for the newly discovered devices from the selected category and manufacturer or **Profile Group**.

For example, If a policy is created for IoT device category with manufacturer or Profile Group with **Auto-Update** Newly Discovered Devices enabled then for any new IoT device discovered with the selected manufacturer, a IoT Access Policy is automatically added to firewall. If port and protocol are specified in the "Device Details" panel, the policy for the newly discovered devices is applied for specified port and protocol.

7. Under Resources, the IoT devices will be auto populated using the Device details configuration described earlier. If the administrator wants to apply policies on different ports for different discovered devices, the port configuration can be edited. If the Admin selects multiple protocol (for example, TCP and UDP) then the device entries appear twice with protocol information in the Resources table. The Admin can choose whether to push the policies for the selected resource based on the IP address, Protocol, and Port information to enforcer by enabling/disabling the checkbox in the resources table.
8. Select the desired Roles for which the policy applies. For example, IoT Administrator.
9. Under Actions, select whether to allow access or deny access.

10. Click **Save Changes**.

IoT Access > IoT Policy Provisioning - Enforcer Policy Configuration > iot-group

iot-group

General

* Name: Required. Label to reference this policy.

Description:

▼ Intranet Enforcer

Platform: JUNOS SRX Palo Alto Networks Firewall

Specify the Intranet Enforcer(s) to which this policy applies. (Applicable for only Juniper and Palo Alto Networks Firewalls.)

Available Enforcers: Selected Enforcers:

▼ Device Details

Specify the filter for getting resources

Category and Manufacturer Profile Group

Click here to configure Device Category or Profile Group.

Select the profile group(s) for which this policy applies.

Available Profile Group(s): Selected Profile Group(s):

Specify Protocol and Port/Range which will be applied to the discovered devices.

Protocol: TCP UDP ICMP

Port: Examples: 80 or 80,433 or 1-1024 or 8080,1-1024,8082 or 1-1024,8080 or 1-100,500-600 etc.

Auto-Update Newly Discovered Devices.

▼ Resources

Resources will be auto-populated using the configuration specified in Device Details panel, port field is editable. Policy for the selected resources will be pushed to enforcer.

10 records per page Search:

IP	Protocol	Port	<input checked="" type="checkbox"/>
10.204.88.72		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.98		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.225		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.226		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.227		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.160		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.69		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.158		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.228		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.193		<input type="text"/>	<input checked="" type="checkbox"/>

Showing 1 to 10 of 24 entries

▼ Roles

Policy applies to ALL roles Policy applies to SELECTED roles Policy applies to all roles OTHER THAN those selected below

Available roles: Selected roles:

▼ Actions

Allow access Deny access

Deny / Reject Message: Short message displayed to users when traffic is denied or rejected. "{SOURCEIP}", "{DESTIP}", "{DESTPORT}", and "{PROTOCOL}" in the message are replaced with the source IP address, destination IP address, destination port, and protocol of the denied traffic. "{USER}" in the message is replaced with the name of the user

NOTE: changes to this page will cause a slight interruption of service for Intranet Enforcer Resource Policies users.

Once the policy is successfully added, it can be viewed as shown in figure.

Policy	Category	Manufacturers	Profile Groups	Auto-Update	Enforcers	Roles	Resources	Action
iot-group			iot-group1	ON	SRX650_89.109 (SRX)	Blocked_Users_Role	10.204.88.72.* 10.204.88.98.* 10.209.114.225.* 10.209.114.226.* 10.209.114.227.* 10.204.88.160.* 10.204.88.69.* 10.204.88.158.* 10.209.114.228.* 10.209.114.193.* More...	Deny
iot-cat	Smartphones/PDAs/Tablets	HUAWAI TECHNOLOGIES CO.,LTD		ON	SRX650_89.109 (SRX)	All roles	10.209.123.81.* 10.204.90.58.* 10.209.122.142.* 10.204.90.73.* 10.209.123.109.* 10.209.123.88.* 10.204.90.23.* 10.209.123.33.* 10.204.90.35.* 10.209.123.31.* More...	Allow



The Device Details panel is only available when IoT Access Policy is created using IoT Policy Provisioning > Enforcer Policy Configuration.

Configuring IoT Access Policy using Palo Alto Networks Firewall

The IoT access policy specifies which users are allowed or denied access to a set of protected resources. You can specify which users you want to allow or deny by choosing the roles for each IoT Access Policy. The IoT Access Policy page enables you to configure the policy based on device details using Profiler device attributes, such as device category and device manufacturer or Profile Group.

When the network Administrator selects category and manufacturer or Profile Group information under device details the IP addresses of the corresponding discovered devices get automatically updated under Resources. Hence the Administrator can seamlessly create IoT Access Policy of profiled devices based on device category, device manufacturer attributes, or Profiler group. If the Administrator wants to have granular control over the IoT devices, further control can be achieved by providing specific port and protocol. The specified port and protocol configuration is applied to all the discovered devices of the selected category and manufacturers.

To configure IoT access policy:

1. Select **Endpoint Policy > IoT Access > IoT Policy Provisioning > Enforcer Policy Configuration**.
2. Click **New Policy**.
3. Enter the Policy name.

4. Enter a description.
5. Under Infranet Enforcer, select the Platform as **Palo Alto Networks Firewall**.
6. Under Security Zones, specify the firewall security zones (source zone/destination zone) for the policy. Multiple zones can be specified with comma separated values. If zones are not specified, then it applies to all zones.
7. Under Service, select any to allow all TCP and UDP ports (default) or select the service to specify the TCP or UDP port or port range. The policy port and protocol configuration remains same for all the resources.

8. Under **Device Details**, specify whether the policy should be applied based on device category and manufacturer or Profile group.

- Category and manufacturer
 - Specify the category from the drop-down list. The values in the drop-down list is populated based on the Device category configuration (IoT Access > IoT Policy Provisioning - Device Configuration).
 - Select the Device manufacturer from the Available Device Manufacturers.
 - Specify the protocol (TCP/UDP) and Port/Range to be applied to the discovered devices.
- Profile Group
 - Configure the Profiler Group (IoT Access > IoT Policy Provisioning - Device Configuration). To configure Profiler Groups, see [Configuring Profiler Groups](#).
 - Select the Profile Group from the Available Profile Groups.
 - Specify the protocol (TCP/UDP) and Port/Range to be applied to the discovered devices.



Port ranges must be configured in dash-separated, comma-delimited, ascending, and non-overlapping order. Multiple port ranges must be separated by a comma. For example, the following examples show the delimiters that are used to enter port ranges:(80, 443, 1-1024, 1-100, 500-600).

The Port/Range entered will be applied to all the discovered devices.

- Select **Auto-Update Newly Discovered Devices** to automatically add IoT Access Policy for the newly discovered devices from the selected category and manufacturer or Profile Group.

For example, If a policy is created for IoT device category with manufacturer or Profile Group with **Auto-Update Newly Discovered Devices** enabled then for any new IoT device discovered with the selected manufacturer, a IoT Access Policy is automatically added to firewall. If port and protocol are specified in the "Device Details" panel, the policy for the newly discovered devices is applied for specified port and protocol.

9. **Under Resources**, the IoT devices will be auto populated using the Device details configuration described earlier. If the administrator wants to apply policies on different ports and protocols for different discovered devices, the port configuration can be edited. If the Admin selects multiple protocol (for example, TCP and UDP) then the device entries appear twice with protocol information in the Resources table. The Admin can choose whether to push the policies for the selected resource based on the IP address, Protocol, and Port information to enforcer by enabling/disabling the checkbox in the resources table.
10. Select the desired Roles for which the policy applies. For example, IoT Administrator.
11. Under **Actions**, select whether to allow access or deny access.

12. Click **Save Changes**.

IoT Access > IoT Policy Provisioning > Enforcer Policy Configuration > New Policy

New Policy

* Name: Required. Label to reference this policy.

Description:

▼ Infranet Enforcer

Platform: JUNOS SRX Palo Alto Networks Firewall

Specify the Infranet Enforcer(s) to which this policy applies.
(Applicable for only Juniper and Palo Alto Networks Firewalls.)

Available Enforcers: Selected Enforcers:

▼ Security Zones

Specify firewall security zones for this policy.
If security zone is not specified, then it applies to all zones i.e. any.
Multiple zones can be specified with comma separated. Example: trust,mgmt

Source Zone: Destination Zone:

▼ Device Details

Specify the filter for getting resources

Category and Manufacturer Profile Group

[Click here to configure Device Category or Profile Group.](#)
Select the profile group(s) for which this policy applies.

Available Profile Group(s): Selected Profile Group(s):

Service:

Auto-Update Newly Discovered Devices.

▼ Resources

Resources will be auto-populated using the configuration specified in Device Details panel. port field is editable.
Policy for the selected resources will be pushed to enforcer.

10 records per page Search:

IP	Protocol	Port	<input checked="" type="checkbox"/>
10.204.88.72		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.98		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.225		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.226		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.227		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.160		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.69		<input type="text"/>	<input checked="" type="checkbox"/>
10.204.88.158		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.228		<input type="text"/>	<input checked="" type="checkbox"/>
10.209.114.193		<input type="text"/>	<input checked="" type="checkbox"/>

Showing 1 to 10 of 24 entries

▼ Roles

Policy applies to ALL roles
 Policy applies to SELECTED roles
 Policy applies to all roles OTHER THAN those selected below

Available roles: Selected roles:

▼ Actions

Allow access
 Deny access

NOTE: changes to this page will cause a slight interruption of service for Infranet Enforcer Resource Policies users.

Once the policy is successfully added, it can be viewed as shown in figure.

IoT Access > IoT Policy Provisioning - Enforcer Policy Configuration

IoT Policy Provisioning - Enforcer Policy Configuration

IoT Policy Provisioning

Basic Configuration | Enforcer Policy Report | **Enforcer Policy Configuration** | Device Configuration

Info: Successfully saved policy:IoT_Group

Show policies that apply to Enforcer: All Enforcers

Showing 1 to 2 of 2 entries records per page

<input type="checkbox"/>	Policy	Category	Manufacturers	Profile Groups	Auto-Update	Enforcers	Roles	Resources	Action
<input type="checkbox"/>	IoT	Internet of Things (IoT)	AMERICAN POWER CONVERSION CORP		ON	pan (PAN)	Users	tcp://10.25.15.11:443 tcp://10.25.15.12:443 tcp://10.25.15.13:443 tcp://10.25.15.14:443 tcp://10.25.15.15:443 tcp://10.25.15.16:443 tcp://10.25.15.177:443 tcp://10.25.15.24:443 tcp://10.204.48.2:443	Allow
<input type="checkbox"/>	IoT_Group			IoT Group	ON	pan (PAN)	Users	tcp://10.204.48.241:443 tcp://10.204.49.21:443 tcp://10.204.49.243:443 tcp://10.204.48.217:443 tcp://10.204.49.122:443 tcp://10.204.49.187:443 tcp://10.204.49.59:443 tcp://10.204.49.30:443 tcp://10.204.49.28:443 tcp://10.204.49.39:443 More...	Allow



Resource Access Policy and IoT Policy Provisioning with Palo Alto Network's Firewall works only with default Virtual System "vsys1" and default device name "**localhost.localdomain**" configuration.

Configuring Additional Device Category/Profile Groups

- The Internet Of Things (IoT) device category is selected by default and hence it is visible by default on IoT policy enforcer report and Policy Configuration page. However, If the Administrator wants to use IoT Policy Provisioning feature for other Profiler supported categories such as Video Conferencing Devices, Printers/Scanners, Medical device, Storage device and so on additional categories can be configured on this page.
- Under Profile Groups, Admin can select the groups that should be used with IoT Policy Provisioning feature. Only the selected Profile Groups are shown while creating IoT access policy using Profile Groups. If none of the Profile Groups are selected in Device Configuration tab then no groups are shown in IoT access policy. To create IoT access policy using Profile Groups, the same needs to be selected in the Device Configuration tab.

IoT Access > IoT Policy Provisioning - Device Configuration

IoT Policy Provisioning - Device Configuration

IoT Policy Provisioning

Basic Configuration | Enforcer Policy Report | Enforcer Policy Configuration | **Device Configuration**

▼ Device Category

Select device categories that will be used for IoT policy provisioning.

<input type="checkbox"/> BSD	<input type="checkbox"/> Datacenter appliance	<input type="checkbox"/> Gaming Consoles	<input type="checkbox"/> Home Audio/Video Equipment	<input checked="" type="checkbox"/> Internet of Things (IoT)	<input type="checkbox"/> Linux
<input type="checkbox"/> Macintosh	<input type="checkbox"/> Medical Device	<input type="checkbox"/> Monitoring Devices	<input type="checkbox"/> Network Boot Agents	<input type="checkbox"/> Other OS	<input type="checkbox"/> Physical Security
<input type="checkbox"/> Point of Sale devices	<input type="checkbox"/> Printers/Scanners	<input type="checkbox"/> Projectors	<input type="checkbox"/> Routers and APs	<input type="checkbox"/> Smartphones/PDAs/Tablets	<input type="checkbox"/> Storage Devices
<input type="checkbox"/> Switches	<input type="checkbox"/> Thin Clients	<input type="checkbox"/> Video Conferencing	<input type="checkbox"/> VoIP Phones/Adapters	<input checked="" type="checkbox"/> Windows	

▼ Profile Group

Select Profile Groups that will be used for IoT Policy Provisioning.

<input checked="" type="checkbox"/> IoT	<input checked="" type="checkbox"/> Network Boot Agents	<input type="checkbox"/> Network Boot Agents-1	<input type="checkbox"/> Operating System
---	---	--	---

[Click here to view or configure Profile Groups.](#)

[Save Changes](#)

Configuring Profiler Groups

Administrator can create different Profile Groups by using different Profiler attributes (for example, group all IoT devices with manufacturer Schneider Electric and Operating System Linux) and combine discovered devices in a group. If an Admin wants to provision IoT Access policy using attributes other than Category and Manufacturer, a Profile Group can be created to group discovered devices and then IoT Policy Provisioning feature can be used for the resources belonging to Profile Group.

To configure Profiler Groups:

1. Select the Profiler server under **Authentication > Auth. Servers**.
2. Select **Profile Groups** tab, select the **New Profile Group**.
3. Enter the **Group Name** and **Rule**. The rules can be written with device attributes and suggested operators can be chosen from the list.

- As an optional step, emails also can be configured which results in notifications for any group related changes.

The screenshot shows the 'Edit Profile Group' interface for the 'IoT' group. The form includes the following fields and options:

- Group Name ***: IoT (with a link 'Devices in this group')
- Rule**: category = "Internet of Things (IoT)"
- Send email notifications whenever a new device enters this group.
- Save** button
- Delete this group** button

- Click **Save Changes**.

Troubleshooting

The event and debug logs can be used for troubleshooting:

- The Event logs are generated whenever the policies are pushed to firewall.
- The Admin Logs are generated upon policy provisioning and auto updation of newly discovered devices.

You can also use **Maintenance > Troubleshooting > Monitoring > Debug Log** for debugging issues.

If the device is not discovered properly in the IoT Policy Provisioning > Enforcer Policy Report page check the Device Discovery Report page for the device category.

The IPS created policies on PAN firewall should not be modified by the PAN admin. The IPS created policies on Palo Alto Networks firewall are tagged as *Pulse Secure Managed*.

Name	Tags	Type	Zone	Source			Destination			Application	Service	Action	Profile	Options
				Address	User	HP Profile	Zone	Address						
1 IoT1	Pulse Secure M	universal	untrust	Users	any	any	trust	10.25.15.60 10.25.15.14	any	IoT3_senic	Allow	none		
2 IoT2	Pulse Secure M	universal	trust	Users	any	any	untrust	10.25.15.60 10.25.15.14	any	any	Deny	none		
3 IoT3	Pulse Secure M	universal	trust	Users	any	any	untrust	10.25.15.60 10.25.15.14	any	IoT3_senic	Allow	none		
4 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none	
5 interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none	none	

Event Logs

To view the communication between IPS and Infranet Enforcer enable **Enforcer Command Trace** under **Events > Settings**.

Log/Monitoring > Events > Log settings

Log settings

Events | User Access | Admin Access | Sensors | Client Logs | SNMP | Statistics | Advanced Settings

Log | Settings | Filters

Save Changes | Reset

Maximum Log Size

Max Log Size: MB

Note: To archive log data, see the [Archiving](#) page.

Select Events to Log

- Connection Requests
- System Status
- System Errors
- Enforcer Events
- License Protocol Events
- IF-MAP Server Trace
- RADIUS Statistics
- Statistics
- Performance
- Enforcer Command Trace

A sample event logs is shown in figure.

Log/Monitoring > Events > Logs

Logs

Events | User Access | Admin Access | Sensors | Client Logs | SNMP | Statistics | Advanced Settings

Log | Settings | Filters

View by filter: Standard/Standard (default) Show 200 items

Edit Query:

Update | Reset Query | Save Query...

Save Log As... | Clear Log | Save All Logs | Clear All Logs

Filter: Standard (default)
Date: Oldest to Newest
Query:
Export Format: Standard

Severity	ID	Message
Info	GWT31691	2018-10-30 03:18:44 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) Commit success: Commit
Info	GWT31691	2018-10-30 03:18:44 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) command: b'<response status="success" code="19"><result><msg><line>Commit job enqueued with jobid 216</line></msg></job216</job></result></response>'
Info	GWT31689	2018-10-30 03:18:43 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) type: commit cmd -<commit></commit>
Info	GWT31691	2018-10-30 03:18:43 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) ADD policy success: IoT
Info	GWT31691	2018-10-30 03:18:43 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) command: b'<response status="success" code="20"><msg>command succeeded</msg></response>'
Info	GWT31609	2018-10-30 03:18:42 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) type: config action: set xpath:/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/rulebase/security/rules/entry[@name='IoT'] element -<tag><member>Pulse Secure Managed</member></tag><source><member>Users</member></source></from><member>untrust</member></from><member>trust</member></to></destination></member>10.25.15.11</member></member>10.25.15.12</member></member>10.25.15.13</member></member>10.25.15.14</member></member>10.25.15.15</member></member>10.25.15.16</member></member>10.25.15.17</member></member>10.25.15.24</member></member>10.204.48.2</member></destination></application><member>any</member></application></service><member>IoT_service_tcp</member></service></action></allow></action>
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) Create source address success: Users
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) command: b'<response status="success" code="20"><msg>command succeeded</msg></response>'
Info	GWT31689	2018-10-30 03:18:42 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) type: config action: set xpath:/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/address-group/entry[@name='Users'] element -<dynamic></filter></Users></filter></dynamic></tag></member>Pulse Secure Managed</member></tag>
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) Create service success: IoT_service_tcp
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) command: b'<response status="success" code="20"><msg>command succeeded</msg></response>'
Info	GWT31689	2018-10-30 03:18:42 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) type: config action: set xpath:/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/service/entry[@name='IoT_service_tcp'] element -<protocol>tcp</port>443</port></protocol></tag></member>Pulse Secure Managed</member></tag>
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) Create tag success: Pulse Secure Managed
Info	GWT31691	2018-10-30 03:18:42 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) command: b'<response status="success" code="20"><msg>command succeeded</msg></response>'
Info	GWT31689	2018-10-30 03:18:41 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) type: config action: set xpath:/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/tag/entry[@name='Pulse Secure Managed'] element -<color>color13</color>
Info	GWT31691	2018-10-30 03:18:41 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) command: b'<response status="success" code="7"></result></response>'
Info	GWT31689	2018-10-30 03:18:41 - ic - [127.0.0.1] System[] - Enforcer.pan(10.204.88.234) type: config action: get xpath:/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/rulebase/security/rules/entry[@name='IoT']

Host Checker

Host Checker Overview

Host Checker is a software component that performs endpoint compliance checks on hosts that connect to the IPS. It supports two types of rules within a policy; predefined and custom. The predefined inspection capabilities consist of health and security checks including antivirus versions, antispyware, OS versions, hard disk encryption status and patch checks. The pre-defined rules are provided by OPSWAT and it uses the ESAP plug-in for pre-defined checks. For more information, see Endpoint Security Assessment Plug-In (ESAP).

Custom rules allows admin to define checks to collect system health using Integrity message collector (IMC) and evaluate using Integrity message verifier (IMV) of TNC framework. The custom rules are created by the admin to include inspection checks such as absence or presence of specific file, certificate checks, TCP ports, processes, registry key settings, NetBIOS name, MAC addresses or certificate of the client machine and third party inspection methods (custom DLLs).

Host Checker evaluation is done at 2 stages:

1. Initial check or evaluation of the user machine as the user browses to the sign-in page.
2. Enforcement of the policy during the user sign-in process, which happens at realm or role level.
 - **Realm-level policies/Pre-Authentication**— The realm level policy is also called as Pre-Authentication requirement as it occurs before the user is prompted for authentication.
 - **Role-level policies/Post-Authentication**—The role level policy is also called as Post-Authentication requirement as it occurs after the user is authenticated and during the role-mapping phase.

If the endpoint does not meet HC policy requirement, administrator can define a customized remediation page with specific instructions and links to resource to ensure that the end user's computer is compliant with the HC policy.

Host checking for layer 2 session is supported only for Pulse initiated 802.1x session. Note that it's not supported for session initiated by native supplicant. For layer 3 sessions host checking is supported for Pulse initiated and browser based sessions.

Trusted Network Connect

Host Checker is compliant with the Trusted Network Connect (TNC) model developed by Trusted Computing Group (TCG). TCG created an architecture and set of standards for verifying endpoint integrity and policy compliance during or after a network access request. For more information about TNC, see www.trustedcomputinggroup.org.

Policies

Ivanti Policy Secure(IPS) Host checker component supports many different type of product policy evaluation on endpoint along with continues monitoring of system health. The below table lists the description of various policies and features, which can be defined as part of device compliance check.

Policy	Description
Predefined	
Antivirus Policy	Policy to detect whether the Antivirus is installed and up-to-date with latest virus signatures. It also includes other options to check the last scan time, virus signature download, and remediation options.
Firewall Policy	Policy to detect the firewall installed on endpoint and the remediation option to turn on the firewall if it's turned off.
Anti-Spyware Policy	Policy to detect the installed spyware on endpoints.
Hard disk Encryption	Policy to detect and check the encryption status of the specified or all drives using installed encryption software.
Patch Management	Policy to check whether the required operating system patches are installed properly.
OS Checks	Policy to check the version of the windows operating systems and minimum service packs.
Common Vulnerability and Exposure (CVE)	Policy to check any vulnerable attacks such as ransomware attack.
System Integrity Protection (SIP)	Policy to check the status (enabled/disabled) of System Integrity Protection (SIP) on the Mac OS endpoints.
Custom	

Policy	Description
3rd Party NHC Check	Policy to specify the location of custom DLL files.
Ports policy	Policy to check if a particular port is either opened or closed to allow or reject the user authentication.
Process policy	Policy to control the software or processes that runs on the client machine.
File Policy	Policy to check if a particular file with specific version or checksum, or last modified file is present on endpoint to allow or reject the user authentication.
Registry Settings policy	Policy to check the registry and its value to allow or reject the user authentication, with a remediation option to set the registry value if not configured.
NetBIOS policy	Policy to check the NetBIOS name from list of NetBIOS names provided to control user access.
MAC Address policy	Policy to check if the endpoint MAC address is in the provided regex or white listing of mac addresses to control user access.
Machine Certificate Policy	Policy to check for the required machine certificate on the endpoint to control user access. This policy evaluates both public and private keys of the installed machine certificate on endpoint for users using Pulse Client. For agentless users, only public key is evaluated.
Advanced Host Checking	<p>Policy to dynamically check the compliance status of the endpoints. It includes combining 2 policy types for obtaining the expected values of the check type. The expected values are fetched from registry location on the client machine for evaluating the policies.</p> <p>The advanced support for checking the expected values against another policy is supported on Ports, Process, File, Registry, NETBIOS, MAC Address, and Machine certificate.</p>
Statement of Health	Policy to perform the health state validation to determine which roles or realms can be accessed by endpoints. It checks the system health indicators such as antivirus is enabled and up to date, antispysware is enabled and up to date, firewall is enabled and so on.
Command	Policy to check the versions of the installed applications on the Mac OS endpoints.

Policy	Description
Host Checker General Settings	IPS provides following admin configuration options while performing host checking.
General Options	
Continuous Policy Evaluation	Option to configure periodic and continuous policy evaluation so that the endpoint is compliant with the Host Checker policy.
Virus Signature Version Monitoring	Option to monitor and verify the virus signatures, operating systems, and patches installed are up to date.
Pre-Authentication Host Checking	Pre-Authentication host checking are policies that are enforced at the realm level before authentication.
Post-Authentication Host Checking	Post-Authentication host checking are policies that are enforced when role assignment happens after authentication.

Agent and Agentless Host Checking

Agentless Host Checking means endpoints trying to connect IPS through browser (User Agent should be a browser such as Google Chrome, Edge, Internet Explorer, Firefox ESR). Agent based Host Checker means endpoints trying to connect to IPS through Pulse Desktop Client (PDC).

You can also see [KB44716](#) for differences between agent and agentless Host Checking.

Agentless	Ivanti Agent
Agentless solution refers to endpoints connecting to network using web browser. With Agentless solution, the device has to get the layer 3 access using an IP address.	Ivanti Agent solution refers to endpoints connecting to network using Pulse Client. With Ivanti agent, the user never gets the full connection to the network during the validation cycle. The connection validations are performed at Layer 2 without requiring the device access the network.

Agentless	Ivanti Agent
Agentless solution polls the network on a regular basis to check whether the endpoint is compliant. The user has to enable security protections at the beginning of the cycle to avoid any network breach.	Ivanti agent always performs continuous monitoring. Any changes to security measures are identified in the real time and thus strengthens the network security posture.
Agentless solution inspects the endpoints using WMI protocol.	Ivanti Agent uses more secured protocols.

Support Platform Matrix

A Host Checker policy contains one or more rules. Each rule can apply to different host checks and for different device types (Windows, Mac, Linux, Solaris, iOS, Android). The below table lists the Host Checker policies that are supported on Windows, Mac, Linux, and Solaris.

Policy	Windows		Macintosh		Linux		Solaris	
	Client	Clientless	Client	Clientless	Client	Clientless	Client	Clientless
Antivirus	Yes	Yes*	Yes	Yes*	No	No	No	No
Firewall	Yes	Yes*	Yes	Yes*	No	No	No	No
AntiSpyware	Yes	Yes	Yes	Yes	No	No	No	No
Hard Disk Encryption	Yes	Yes	Yes	Yes	No	No	No	No
Patch Assessment	Yes	Yes	Yes	Yes	No	No	No	No
OS Checks	Yes	Yes	Yes	Yes	No	No	No	No
Common Vulnerability	Yes	Yes	No	No	No	No	No	No

Policy	Windows		Macintosh		Linux		Solaris	
and Exposure (CVE) Check								
3rd Party NHC Checks	Yes	Yes	No	No	No	No	No	No
Ports	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Files	Yes	Yes**	Yes	Yes**	Yes	Yes**	Yes	Yes**
Registry Setting	Yes	Yes***	No	No	No	No	No	No
NetBIOS	Yes	Yes	Yes	Yes	No	No	No	No
MAC Address	Yes	Yes	Yes	Yes	No	No	No	No
Machine Certificates	Yes	Yes****	Yes	Yes	No	No	No	No
Statement of Health	Yes	Yes	No	No	No	No	No	No
System Integrity Protection (SIP)	No	No	Yes	Yes	No	No	No	No
Command	No	No	Yes	Yes	No	No	No	No
Advanced Host Checking	Yes	Yes	No	No	No	No	No	No

- * In some occasions, Antivirus/Firewall products restricts the remediation actions to admin/services (For example but not limited to, turning on firewall). In such scenarios, certain remediation actions won't work with browser/clientless logins. Note that, this is defined by the corresponding security products.

- **Admin should enable system level access for accessing certain files and file locations for browser login.



- ***To access device-certificates from system store, the plugin needs admin rights. With browser/clientless login private key verification is not supported in Agentless login.

- ****Registry verification requires admin privileges for accessing certain registry files. There are limitations with accessing some of the registry hierarchy for evaluating registry checks for browser login.

- Agentless mode with Profiler is supported only with Windows platforms. The supported policies are Antivirus, Firewall, Antispyware, OS checks, Ports, Process, NetBIOS, and MAC Address. For more information, see Profiler documentation.

Host Checker Remediation Capabilities

	Windows	Mac OS	Linux
Custom Instructions	Yes	Yes	Yes
Custom Actions	Yes	-	-
Kill Process	Yes	Yes	Yes
Delete Files	Yes	Yes	Yes
Reason String	Yes	Yes	Yes

Host Checker Installation Options

Host Checker is supported for agent and agentless clients. The installation options are listed below:

- Browser based Host Checking (Agentless) — This is used for browser-based logins and requires PSAL to be present on the endpoint. If PSAL is not available on the endpoint, it gets installed as part of the connection.

- It is recommended not to keep a very low value for **login inactivity timeout** (For example, 1 or 2 minutes). This might result in connection timeouts on fresh endpoints where PSAL also need to be installed as part of compliance evaluation.
- Pulse Client (Agent)—You can use Pulse client, which contains the Host Checker component for compliance check. To manually install the Host Checker, Select **Maintenance > System > Installers** and download the Pulse installer.

Using the downloaded executable file, you can:

- Distribute the file to client machines using software distribution tools. This option enables you to install an application or service on client machines.
- Post the executable in a secure repository so that users with the proper administrator right may download and install the appropriate version.

Auto-upgrading Host Checker

To automatically upgrade Host Checker:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Under Options, select **Auto-upgrade Host Checker** if you want the system to automatically download the Host Checker application to a client computer when the version of Host Checker on the system is newer than the version installed on the client.
3. Click **Save Changes**.

Endpoint Security Assessment Plug-In (ESAP)

The Endpoint Security Assessment Plug-in (ESAP) is a plug-in in IPS using which you can upload the latest SDK from Opswat independently.

Ivanti frequently adds enhancements, bug fixes, and support for new third-party applications to the plug-in. New plug-in releases are available independently and more frequently than new releases of the system software package. If necessary, you can upgrade the plug-in independently of a system upgrade.

You can upload up to four versions of the plug-in, but the system uses only one version at a time (called the active version). If necessary, you can rollback to a previously active version of the plug-in.

If the endpoints in your deployment connect to multiple servers simultaneously, all of those connected servers must use the same version of the ESAP plug-in.

Upgrading the ESAP

1. To upgrade the ESAP plug-in:
 - Download the Endpoint Security Assessment Plug-in from the [Ivanti Support Portal](#).
 - To access the Customer Support Center, enter a username and password for a Ivanti Support Center account.
 - Click the ESAP Download Page link.
 - Navigate to the ESAP release you want.
 - Download the plug-in zip file to your computer.
2. Select **Authentication > Endpoint Security > Host Checker**.
3. On the Host Checker page, under Manage Endpoint Security Assessment Plug-In Versions:
 - If you want IPS to actively begin using the new component software immediately after you upload it, select the Set as active after upload option.
 - Click **Browse**, select the plug-in file to upload and click **OK**.
 - Click **Upload**. After the plug-in is installed, the date and time of the plug-in installation is displayed in the plug-in list.
 - If you did not select the Set as active after upload option, activate the plug-in to use by selecting the version in the plug-in, list and click **Activate**.

- You can rollback to an older plug-in version after you upgrade to a later version by selecting the older version as the active version.



- If you upgrade the system software to a newer version, or if you import a user configuration file, active plug-in version can change based on the supportability of ESAP version. If you want to use a different plug-in version after you upgrade or importing a user configuration file, you must manually activate that plug-in version.

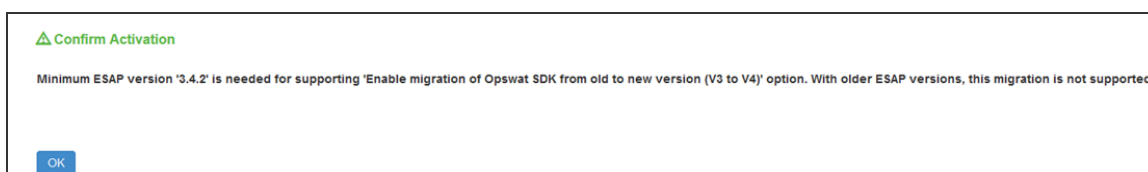
OPSWAT SDK V3 to V4 Migration

Ivanti supports Opswat version 3 and version 4 for endpoint compliance evaluation. The migration option helps the administrators to migrate their servers and clients with Opswat v4 to take advantage of latest updates.

Software Support- Starting with Release 9.1R2 and later releases.

OS support: Windows 7 and later releases and macOS 10.12 and later releases

Prerequisites - ESAP 3.4.2 is the minimum version. A warning message is displayed if the minimum version is not present.



Procedure to migrate from Opswat V3 to V4

To migrate follow the below procedure:

1. Navigate to **“Manage Endpoint Security Assessment PlugIn Versions”** section on **Authentication > Endpoint Security > Host Checker page.**
2. Enable the option for **Enable migration of Opswat SDK from old to new version (V3 to V4).**
3. On enabling this option, the clients start downloading the **V4 SDK and migrate to newer SDK.**

Manage Endpoint Security Assessment PlugIn Versions

Currently Active ESAP version: 3.4.2
Default ESAP version: 3.3.5

10 records per page

Version	Uploaded	Last Activated
3.3.5	Fri Jun 14 00:19:55 2019	Mon Jun 17 13:04:54 2019
3.4.2	Mon Jun 17 12:47:52 2019	Mon Jun 17 13:05:11 2019

Enable migration of Opswat SDK from old to new version (V3 to V4)

Note: Enabling this option starts Opswat SDK V3 to V4 migration on the client machines. This option enforces V3 Opswat SDK usage in host checker policy definitions by enabling Older SDK usage option below, so that host check happens properly irrespective of whether client machine has Opswat V3 or V4 SDK installed. During the next host check on the client machine, Opswat V4 SDK will be installed. Minimum ESAP version '3.4.2' is needed for supporting this migration.

Activate Older Opswat SDK in ESAP for Host checker policy evaluation.

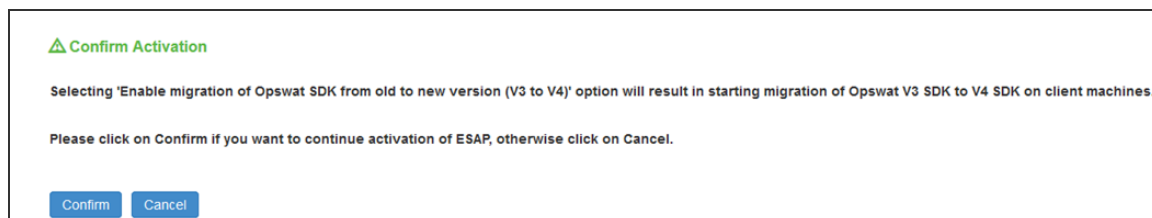
Note: ESAP contains two versions of Opswat SDKs for supporting policy evaluation. It is recommended to use the newer version of the Opswat SDK. Use the older version if you have Pulse Clients before 5.2R5, Pulse Connect Secure appliances before 6.2R5, or Pulse Policy Secure appliances before C9.3R5.

Enable Active ESAP package on the client

Note: Enabling this option ensures that the active ESAP package is used on all the client machines. If the client machine contains a newer ESAP package it will be replaced with the active ESAP version.

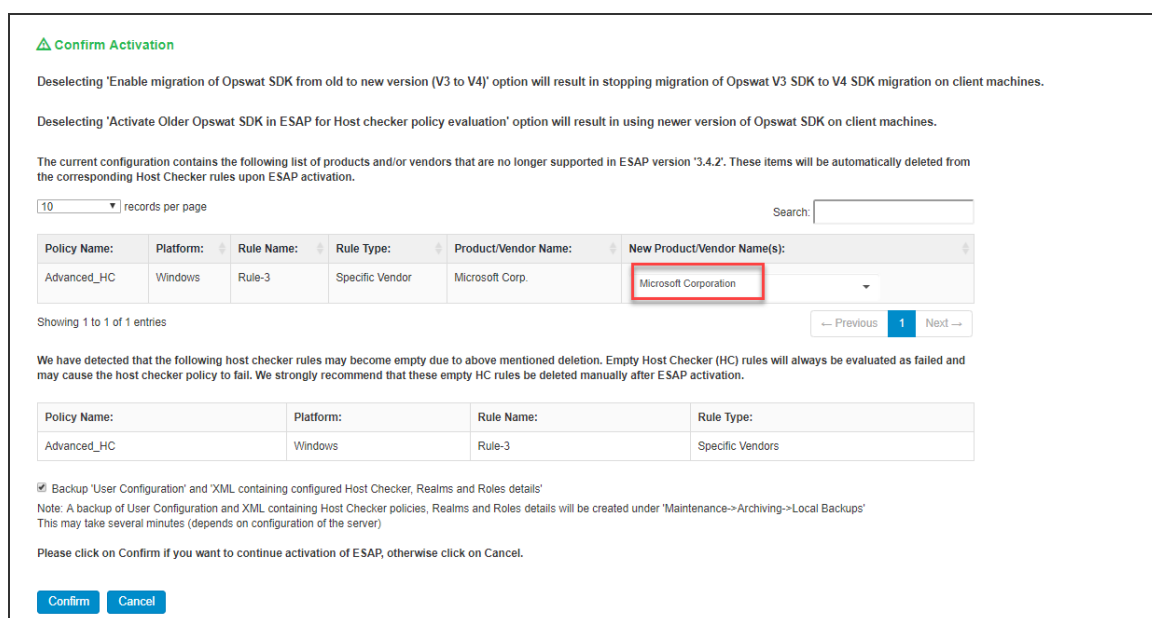
Package No file chosen Set as active after upload

4. **Uncheck/Disable Enable migration of OPSWAT SDK from old to new version (V3 to V4)** option once the migration is complete. Verify the migration status.
5. A confirmation message display. Click **Confirm**.



Post migration, Admin can remap the configured products in the policies to map to the newer SDK using the post migration window.

For example, in the below screenshot the Product /Vendor Name for the policy has been changed from Microsoft Corp. to Microsoft Corporation for successful migration.



6. Enable **Backup User Configuration** and XML containing **Host Checker, Realms** and **Role details for performing configuration backup**. This option helps to revert to the previous version of IPS/ICS configuration, if required.
7. Click **Confirm**.

Compliance Report

The Compliance Report displays the compliance details of the users connected to the server. The report also includes the Opswat SDK Version used for these connections. **Opswat SDK Version** is used to filter the users using a specific Opswat SDK version.

The compliance report page displays the Opswat SDK version details only when "Enable migration of OPSWAT SDK from old to new version (V3 to V4)" option is enabled.

To check the SDK version for each connection, view the report under **System > Reports > Compliance Report**.

Compliance Report Download Report: CSV | Tab Delimited

Filter by: Date Range: Last 24 Hours

Compliance Results: Compliant Non-Compliant Remediated Not-Assessed

Opswat SDK Version: All

Username:

Realm:

MAC Address:

Apply Filter

View: 10

Username	Realm	Device ID	MAC Address	Session Compliance	Initial Host Check Time	Initial Host Check Details
useron130	Users		00-50-56-BF-2A-9D	Remediated	Mon Jun 17 14:29:54 2019	Host check result: Pass Opswat SDK Version: V4
useron130	Users		00-50-56-BF-2A-9D	Remediated	Mon Jun 17 14:28:28 2019	Host check result: Fail Failed Policies: • Advanced_HC Failure reasons: • Firewall not running Opswat SDK Version: V4

Roll back procedure

To roll back to previous version of Opswat SDK:

1. Navigate to **"Manage Endpoint Security Assessment PlugIn Versions"** section on **Authentication > Endpoint Security > Host Checker** page.
2. Uncheck **Enable migration of Opswat SDK from old to new version (V3 to V4)**.
3. Enable **Activate Older Opswat SDK in ESAP for Host Checker** policy evaluation.

4. Click **Save ESAP changes**.

Manage Endpoint Security Assessment Plugin Versions

Currently Active ESAP version: 3.4.2
Default ESAP version: 3.3.5

10 records per page

Version	Uploaded	Last Activated
3.3.5	Fri Jun 14 00:19:55 2019	Mon Jun 17 13:04:54 2019
3.4.2	Mon Jun 17 12:47:52 2019	Mon Jun 17 14:30:23 2019

Delete
 Enable migration of Opswat SDK from old to new version (V3 to V4)
 Activate Older Opswat SDK in ESAP for Host checker policy evaluation
 Enable Active ESAP package on the client
 Set as active after upload

Package: No file chosen Set as active after upload

End User Flow

User logging in from browser or User logging in from Pulse client for L3 connection

- Client machine has Opswat V3 SDK installed.
- Host Check starts on the client machine as part of connection establishment.
- Server sends the required information to client for upgrading V3 to V4 SDK.
- Client downloads V4 SDK and collects the installed security products details using newly installed V4 SDK and sends the detected product details to server.
- Server evaluates configured Opswat based rules by consuming the details received from client machine.
- Host Checker continues to use the installed V4 SDK on client machine for subsequent host checks and connections.

User logging in from Pulse client for L2 connections

- Client machine has Opswat V3 SDK installed.
- Host Check starts on the client machine as part of connection establishment.
- Server sends the required information to client for upgrading V3 to V4 SDK.
- During L2 connection, client fails to download V4 SDK.
- Host Checker collects the installed security products details using existing V3 SDK and sends the detected product details to server.

-
- Server evaluates configured Opswat based rules by consuming the details received from client machine.
 - L2 connection is established followed with an L3 connection.
 - Server detects L2 followed by L3 connection attempt and remembers that ESAP upgrade is needed on the client machine.
 - Host Check is triggered again on client machine during L3 connection.
 - Server sends the required information to client for upgrading V3 to V4 SDK.
 - Client downloads V4 SDK (because L2 connection is complete already) and collects the installed security products details using newly installed V4 SDK and sends the detected product details to server.
 - Server evaluates configured Opswat based rules by consuming the details received from client machine.
 - Host Checker continues to use the installed V4 SDK on client machine for subsequent host checks and connections.



Host checking is done twice for the same client machine (once during L2 connection and once during L3 connection) for the first time. However, Host Checking is done only once for the subsequent connections as the client machines has the Opswat V4 SDK installed.

Activating the Opswat SDK Version

Beginning with Release 5.3R5, IPS supports both v3 and v4 SDKs provided by OPSWAT. The default SDK version used is v4, but it can be reconfigured based on your requirement. The product/vendor names used by v3 and v4 SDK might differ. Due to the product/vendor names mismatch, there is a possibility that the rules become empty while creating Host Checker rule with v3 SDK activated and upon enabling v4 SDK. To avoid this, a migration page is added to help the administrators in migrating the policies from v3 to v4 SDK.

To use v3 or v4 SDK:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Enable the **Activate Older SDK in ESAP for Host Checker policy evaluation** check box for v3 SDK.

3. Disable the **Activate Older SDK in ESAP for Host Checker policy evaluation** check box for v4 SDK.

▼ Manage Endpoint Security Assessment Plugin Versions

Currently Active ESAP version: 3.3.2
Default ESAP version: 3.3.2

10 records per page Search:

Version	Uploaded	Last Activated
<input type="radio"/> 3.2.7	Wed Sep 26 13:52:14 2018	Wed Sep 26 13:52:54 2018
<input checked="" type="radio"/> 3.3.2	Thu Jan 17 15:07:13 2019	Thu Jan 17 15:07:15 2019

← Previous 1 Next →

Activate Older Opswat SDK in ESAP for Host checker policy evaluation.

Note: ESAP contains two versions of Opswat SDKs for supporting policy evaluation. It is recommended to use the newer version of the Opswat SDK. Use the older version if you have Pulse Clients before 5.2R5, Pulse Connect Secure appliances before 6.2R5, or Pulse Policy Secure appliances before 6.3R5.

Enable Active ESAP package on the client

Note: Enabling this option ensures that the active ESAP package is used on all the client machines. If the client machine contains a newer ESAP package it will be replaced with the active ESAP version.

Package: No file chosen Set as active after upload

* Indicates required field



It is recommended to disable this option for using newer version of OPSWAT SDK, after all the Pulse Clients are upgraded to 5.2R5 or above and servers are upgraded to IPS 5.3R5 or above.

4. Click **Save ESAP Changes**. A confirm Activation page appears which lists the products and/or vendors, which are no longer supported in that particular ESAP SDK version. From the drop downlist, admin can select one or many new products /vendors instead of the existing product/vendor.

Confirm Activation

The current configuration contains the following list of products and/or vendors that are no longer supported in ESAP version '3.0.1'. These items will be automatically deleted from the corresponding Host Checker rules upon ESAP activation.

10 records per page Search:

Policy Name:	Platform:	Rule Name:	Rule Type:	Product/Vendor Name:	New Product/Vendor Name(s):
Hc_check	Mac	av	Specific Vendor	Kaspersky Labs	Kaspersky Lab
		firewall	Specific Vendor	Apple Computer, Inc.	
	Windows	antivirus	Specific Vendor	Microsoft Corp.	
		firewall	Specific Product	Microsoft Windows Firewall (10.x)	
		hd	Specific Product	Symantec Encryption Desktop (10.x)	
			Specific Vendor	Symantec Corp.	
		patch	Specific Product	System Center Configuration Manager (5.x)	

Showing 1 to 7 of 7 entries

← Previous 1 Next →

- Only the products/vendors, which get changed are listed. If some rules have some products/vendors whose names are not changed, those products/vendors will be automatically migrated and will not be listed.



- When the ESAP version is changed from upper version to lower version and if any product is not listed in the selected ESAP version, then the backup configuration will not work.

5. Enable **Backup 'User Configuration' and 'XML containing configured Host Checker, Realms and Roles details** check box to create a local backup of user configurations under **Maintenance > Archiving > Local Backups**.

evaluated as failed and may cause the host checker policy to fail. We strongly recommend that these empty HC rules be deleted manually after ESAP activation.

Policy Name:	Platform:	Rule Name:	Rule Type:
Hc_check	Mac	av	Specific Vendors
		firewall	Specific Vendors
	Windows	firewall	Specific Products
		hd	Specific Products
			Specific Vendors
		patch	Specific Products

Backup 'User Configuration' and 'XML containing configured Host Checker, Realms and Roles details'

Note: A backup of User Configuration and XML containing Host Checker policies, Realms and Roles details will be created under 'Maintenance->Archiving->Local Backups'
This may take several minutes (depends on configuration of the server)

Please click on Confirm if you want to continue activation of ESAP, otherwise click on Cancel.



Server maintains a maximum of 5 backups. To capture a new backup, older backup will be automatically deleted.

6. Click **Confirm**.

Changing the Active ESAP Package

Administrator can activate any of the already uploaded ESAP packages by selecting the corresponding radio button under "Manage Endpoint Security Assessment Plugin Versions" table and then clicking on "Save ESAP Changes" button.

To change the active ESAP packages:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Under **Manage Endpoint Security Assessment Plugin Versions**, select the required ESAP version.

3. Click **Save ESAP Changes**.

Manage Endpoint Security Assessment Plugin Versions

Currently Active ESAP version: 3.3.2
Default ESAP version: 3.3.2

10 records per page Search:

Version	Uploaded	Last Activated
<input type="radio"/> 3.2.7	Wed Sep 26 13:52:14 2018	Wed Sep 26 13:52:54 2018
<input checked="" type="radio"/> 3.3.2	Thu Jan 17 15:07:13 2019	Thu Jan 17 15:07:15 2019

-- Previous **1** Next --

Activate Older Opswat SDK in ESAP for Host checker policy evaluation.
Note: ESAP contains two versions of Opswat SDKs for supporting policy evaluation. It is recommended to use the newer version of the Opswat SDK. Use the older version if you have Pulse Clients before 5.2R5, Pulse Connect Secure appliances before 8.2R5, or Pulse Policy Secure appliances before C3.3R5.

Enable Active ESAP package on the client
Note: Enabling this option ensures that the active ESAP package is used on all the client machines. If the client machine contains a newer ESAP package it will be replaced with the active ESAP version.

Package: No file chosen Set as active after upload

* Indicates required field



If the client machine has newer ESAP package and if it has to be replaced, then select “Enable the Active ESAP package”. See [Enabling the Active ESAP Package](#) to know about the procedure.

Enabling the Active ESAP Package

Administrator can enable “Enable Active ESAP package on the client” checkbox to ensure that client machine always uses the active ESAP package, even if the active ESAP package is older than the version installed on the client system. In case client machine has newer ESAP package installed, it will be replaced with the older Active ESAP version with this option enabled.

To enable the active ESAP package:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Under **Manage Endpoint Security Assessment Plugin Versions**, enable Enable Active ESAP package on the client checkbox.

▼ Manage Endpoint Security Assessment Plugin Versions

Currently Active ESAP version: 3.3.2
Default ESAP version: 3.3.2

10 records per page

Version	Uploaded	Last Activated
<input type="radio"/> 3.2.7	Wed Sep 26 13:52:14 2018	Wed Sep 26 13:52:54 2018
<input checked="" type="radio"/> 3.3.2	Thu Jan 17 15:07:13 2019	Thu Jan 17 15:07:15 2019

[Delete](#)

Activate Older Opswat SDK in ESAP for Host checker policy evaluation.
Note: ESAP contains two versions of Opswat SDKs for supporting policy evaluation. It is recommended to use the newer version of the Opswat SDK. Use the older version if you have Pulse Clients before 5.2R5, Pulse Connect Secure appliances before 8.2R5, or Pulse...

Enable Active ESAP package on the client
Note: Enabling this option ensures that the active ESAP package is used on all the client machines. If the client machine contains a newer ESAP package it will be replaced with the active ESAP version.

Package: [Browse](#) No file chosen [Upload](#) Set as active after upload

[Save ESAP Changes](#)

3. Click **Save ESAP Changes**.

Updating Virus Signature Database

You can automatically import the current virus-signature version-monitoring from the Ivanti staging site at a specified interval, or you can download the files from Ivanti portal and use your own staging server. You can also configure a proxy server as a staging site between IPS and the Ivanti site. To use a proxy server, you enter the server network address, port, and authentication credentials, if applicable.

To access the Ivanti staging site for updates, you must enter the credentials for your Ivanti Support account.

For patch assessment remediation with Ivanti you can use OPSWAT (a third-party vendor) to automatically download patches from trusted sources to the endpoint.

To configure IPS to automatically import the current virus signature version-monitoring from the Ivanti staging site:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Select **Virus signature version monitoring**.
3. Select **Auto-update virus signatures list**.

4. For Download path, leave the existing URLs of the staging sites where the current lists are stored. The default URLs are the paths to the Ivanti staging site:
5. For Download interval, specify how often you want IPS to automatically import the current list(s).
6. For Username and Password, enter your Ivanti Global Support Center credentials.
7. Click **Save Changes**.

To manually import the current virus signature version-monitoring lists:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Click **Virus signature version monitoring**.
3. Download the list(s) from the Ivanti staging site to a network server or local drive on your computer by entering the Ivanti URLs in a browser window:
 - https://download.pulsesecure.net/software/av/uac/epupdate_hist.xml
 - <https://download.pulsesecure.net/software/hc/patchdata/patchupdate.dat>
4. Under **Manually import virus signatures** list, click **Browse**, select the list, and then click **OK**.
5. Click **Save Changes**.



If you use your own staging site for storing the current list(s), you must upload the trusted root certificate of the CA that signed the staging's server certificate to IPS.

To use a proxy server as the auto-update server:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Select **Virus signature version monitoring**.
3. Select **Auto-update virus signatures list**.

4. For Download path, leave the existing URLs of the staging sites where the current lists are stored. The default URLs are the paths to the Ivanti staging site:
 - https://download.pulsesecure.net/software/av/uac/epupdate_hist.xml
(for auto update virus signatures list)
 - <https://download.pulsesecure.net/software/hc/patchdata/patchupdate.dat>
(for auto update patch management)
5. For Download interval, specify how often you want IPS to automatically import the current lists.
6. For Username and Password, enter your Ivanti Global Support Center credentials.
7. Select the **Use Proxy Server** check box.
8. For IP Address, enter the IP address of your proxy server.
9. For Port, enter the port that the Ivanti Global Support Center will use to communicate with your proxy server.
10. If your proxy server is password protected, type the Username and Password of the proxy server.
11. Click **Save Changes**.

Understanding Host Checker Policy Remediation

This topic describes Host Checker policy remediation.

Remediation Options

You can specify general remediation actions for Host Checker to take if an endpoint does not meet the requirements of a policy. For example, you can display a remediation page to the user that contains specific instructions and links to resources to help the user bring their endpoint into compliance with Host Checker policy requirements.

You can also include a message to users (called a reason string) that is returned by Host Checker or an IMV and that explains why the client machine does not meet the Host Checker policy requirements.

For example, the user might see a remediation page that contains custom instructions, a link to resources, and reason strings:

For each Host Checker policy, you can configure two types of remediation actions:

- **User-driven**—Using custom instructions and reason strings, you can inform the user about the failed policy and how to make his computer conform. The user must take action to successfully re-evaluate the failed policy unless you configure an IMV to automatically remediate his computer. For instance, you can create a custom page that is linked to a policy server or Web page and enables the user to bring his computer into compliance.
- **Automatic (system-driven)**—You can configure Host Checker to automatically remediate the user's computer. For example, when the initial policy fails, you can kill processes, delete files, or allow automatic remediation by an antivirus rule, a firewall rule, or a registry setting rule. Host Checker does not inform users when performing automatic actions. (You could, however, include information in your custom instructions about the automatic actions.)

Remediation User Experience

Users might see a remediation page in the following situations:

- Before the user signs in:
 - If you enable custom instructions or reason strings for a policy that fails, the system displays the remediation page. The user has two choices:
 - Take the appropriate actions to make the endpoint conform to the policy and then click **Try Again** on the remediation page. Host Checker checks the user's computer again for compliance with the policy.
 - Leave the endpoint in its current state and click **Continue** to sign in. The user cannot access the realm, role, or resource that requires compliance with the failed policy.

If you do not configure the system with at least one realm that allows access without enforcing a Host Checker policy, the user must bring the endpoint into compliance before signing in.

- If you do not enable custom instructions or reason strings for a policy that fails, Host Checker does not display the remediation page. Instead, a message displays telling the user that no additional information has been provided and to contact the system administrator. The system does not assign the user a role that allows access to protected resources.

- After the user signs in:
 - **Pulse**—During a session, if a user's computer becomes noncompliant with the Host Checker policy, a message is displayed briefly in the system tray that informs the user of the noncompliance. The remediation page is displayed on the client.
 - **Agentless**—During a session, if a user's agentless computer becomes noncompliant with the Host Checker policy, the system displays the remediation page to inform the user of the noncompliance. On Windows agentless computers, Host Checker displays a bubble and tray icon if the endpoint becomes noncompliant. The user must click the bubble or tray icon to open a browser window that contains the remediation instructions. On Macintosh, Linux or Solaris agentless computers, Host Checker automatically opens a browser window that contains the remediation instructions as soon as the endpoint is noncompliant.

Configuring Host Checker Policy

To configure a Host Checker policy:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Under Policies, click **New**.
3. Enter a name in the Policy Name field then click Continue. (Users see this name on the Host Checker remediation page if you enable custom instructions for this policy.)
4. Create one or more rules to associate with the policy.
5. Configure additional system-level options on **Authentication > Endpoint Security > Host Checker page**.

6. Determine the level at which you want to enforce Host Checker policies:
 - To enforce Host Checker policies when the user initially signs in, implement the policy at the realm level select **Users > User Realms > Select Realm > Authentication Policy > Host Checker**.
 - To allow or deny users access to specific roles based on compliance with Host Checker policies, implement the policies at the role level by using the **Users > User Roles > Select Role > General > Restrictions > Host Checker** page of the admin console.
 - To map users to roles based on their compliance with Host Checker policies, select **Users > User Realms > Select Realm > Role Mapping** and use custom expressions.
7. To create client-side logs. Select **System > Log/Monitoring > Client Logs/Settings and enable Host Checker** and **Pulse Desktop Client** option.
8. If more than one valid session exists from the same system, and Host Checker is used in those sessions, all valid sessions are terminated if a user signs out from any of the sessions. To prevent this, turn off Host Checker for those sessions that do not need Host Checker.



Enable **Agentless Mode with Profiler** for using Agentless Host Checker policy evaluation. As a pre-requisite the Admin must configure the Profiler server to collect the endpoint attributes. Note that the Agentless Mode with Profiler functionality is also supported on the MAC Authentication Realm. Refer the Profiler documentation for configuration and other details.

Configuring Antivirus Rule with Remediation Options

Use this rule type to configure antivirus rule along with remediation actions. You can also monitor policies to ensure that logged-in endpoints maintain compliance status, and remediate the endpoint to another role or realm depending on the current status.

To configure a predefined antivirus rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a policy or click on existing policy in the Policies section of the page.
3. Select the tab for Windows or Mac, depending on the platform for which this rule is intended.

- Under Rule Settings, select **Predefined: Antivirus** and click **Add**.

Configuration > Host Checker Policy > Add Predefined Rule : Antivirus

Add Predefined Rule : Antivirus

Rule Type: Antivirus

*Rule Name:

▼ *Criteria

- Require any supported product.
- Require specific products/vendors
- Require any supported product from a specific vendor.
- Require specific products

▼ Optional

The following check is supported by [these Antivirus products](#). For any other products, this check will be ignored.

- Successful System Scan must have been performed in the last days.

The following check is supported by [these Antivirus products](#). For any other products, this check will be ignored. For this check to be effective, enable the 'Auto-update virus signatures list' option or manually import the virus signatures list on Endpoint Security page.

- Check for the Virus Definition files

- Monitor this rule for change in result

Note: Enabling this option will report change in compliance for this rule to the Pulse Policy Secure immediately. The client component requires additional computing cycles to report change in compliance immediately. We strongly recommend that this option be enabled for rules that are dynamic in nature, for example a rule for RTP check provided by Antivirus software. For other rules the host checker update frequency should be used to get periodic health checks from endpoints.

Powered by **OPSWAT**

- Enter the name of the antivirus rule.
- To determine if your software vendor's product is supported for the System Scan check, click **these Antivirus products**. A new window opens with a list of the products that support the feature.
- Select or clear the check box next to **Successful System Scan must have been performed in the last _ days**, and enter the number of days in the box. If you select this check box, a new option is displayed. If the remediation action to start an antivirus scan successfully begun, you can override the previous check.
- Select or clear **Consider this rule as passed if 'Full System Scan' was started successfully as remediation** check box.
- Select or clear the **Check for Virus Definition files** check box. If you select this check box, then choose either **Virus Definition files should not be older than n Updates** (the range for this value is 1 - 20) or Virus Definition files should not be older than n Days (the range for this value is 1 – 30).

10. Select one of the following options:

- **Require any supported product** allows you to check for any product (rather than requiring you to select every product separately). This option button reveals a list of products in the remediation section to allow you to enable remediation options which are product specific.
- **Require specific products/vendors** allows you to define compliance by allowing any product by a specific vendor or provides functionality that allows you to select individual products to define compliance.

After you select your vendors and products, remediation options appear on the page.

For each of the following remediation actions:

- **Download latest virus definition files**—Obtains the latest available file for the specified vendor from the vendor's website.
- **Turn on Real Time Protection**—Launches the virus-scanning mechanism for the specified vendor.
- **Start Antivirus Scan**—Performs a real-time virus scan for the specified vendor.

The check box is active if the action is supported for your product.

If your antivirus product is not supported, you can click the remediation column headers to determine what vendors and products are supported.

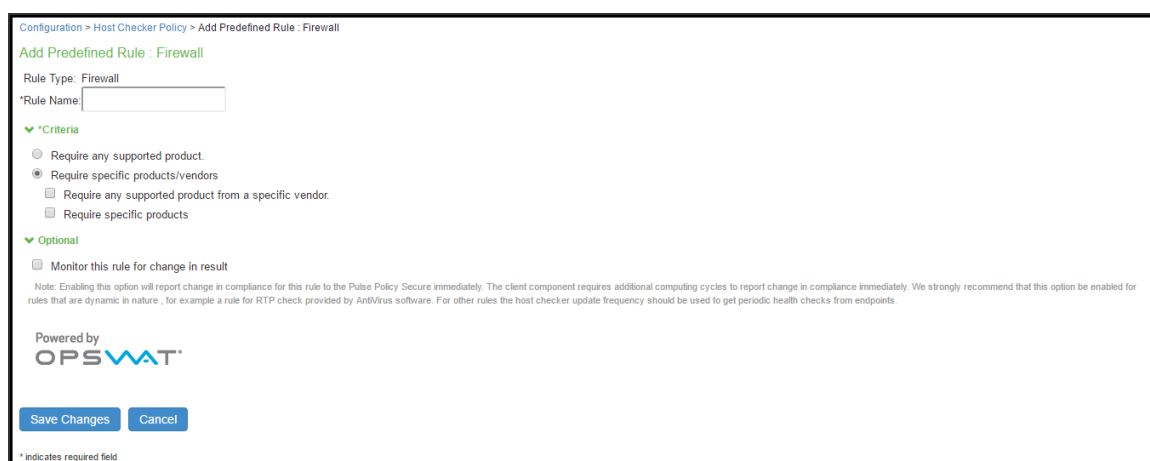
- If your product is supported, select the check box for the remediation action that you want to apply.
- Under Optional, select **Monitor this rule for change** in result to continuously monitor the policy compliance of endpoints. If this check box is selected, the compliance status of an endpoint that has successfully logged in changes, IPS initiates a new handshake to reevaluate realm or role assignments.
- Click **Save Changes** to save the antivirus rule and enforce antivirus remediation.
- (Optional) Add more rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

Configuring Firewall Rule with Remediation Options

Use this rule type to create a Host Checker firewall rule that requires the endpoint to have a specific firewall installed and running before it connects to the network.

To configure a Host Checker predefined firewall rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a policy or click an existing policy in the Policies section of the page.
3. Select the tab for Windows or Mac, depending on the platform for which this rule is intended.
4. Under Rule Settings, select **Predefined: Firewall** and **click Add**.



The screenshot shows the 'Add Predefined Rule: Firewall' configuration page. The breadcrumb trail is 'Configuration > Host Checker Policy > Add Predefined Rule: Firewall'. The page title is 'Add Predefined Rule: Firewall'. The 'Rule Type' is set to 'Firewall'. There is a text input field for '*Rule Name'. Under the 'Criteria' section, there are four radio button options: 'Require any supported product', 'Require specific products/vendors' (which is selected), 'Require any supported product from a specific vendor', and 'Require specific products'. Under the 'Optional' section, there is a checkbox for 'Monitor this rule for change in result'. A note at the bottom states: 'Note: Enabling this option will report change in compliance for this rule to the Pulse Policy Secure immediately. The client component requires additional computing cycles to report change in compliance immediately. We strongly recommend that this option be enabled for rules that are dynamic in nature, for example a rule for RTP check provided by Antivirus software. For other rules the host checker update frequency should be used to get periodic health checks from endpoints.' The page is powered by OPSWAT and has 'Save Changes' and 'Cancel' buttons at the bottom. A small asterisk indicates required fields.

5. Enter a name for the firewall rule.
6. Select one of the following options:
 - **Require any supported product** allows you to check for any product (rather than requiring you to select every product separately). This option button provides a list of products in the remediation section to allow you to enable remediation options which are product specific.
 - **Require specific products/vendors** allows you to define compliance by allowing any product by a specific vendor or provides functionality that allows you to select individual products to define compliance.
7. After you select your vendors and products, remediation options appear on the page.
8. If your firewall is supported, select the **Turn on Firewall** check box.

9. Under Optional, select **Monitor this rule for change** in result to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, IPS initiates a new handshake to reevaluate realm or role assignments.
10. Click **Save Changes** to save the firewall rule and enforce firewall remediation.
11. (Optional) Add more rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

Configuring Malware Rule

Use this rule type to check for installed malware on endpoints.

To configure a Host Checker Predefined malware rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new or click an existing policy in the Policies section of the page.
3. Select the tab for Windows.
4. Under Rule Settings, select **Predefined: Malware** and **click Add**.



5. From the Criteria, select the **Malware Software** to be installed on the endpoint.
6. Click **Save Changes**.

Configuring AntiSpyware Rule

Use this rule type to check for installed antispyware on endpoints.

To configure a Host Checker Predefined Spyware rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new or click an existing policy in the Policies section of the page.
3. Select the tab for Windows or Mac, depending on the platform for which this rule is intended.
4. Under Rule Settings, select **Predefined: AntiSpyware** and **click Add**.

Configuration > Host Checker Policy > Add Predefined Rule: AntiSpyware

Add Predefined Rule: AntiSpyware

Rule Type: AntiSpyware

*Rule Name:

▼ *Criteria

Note: Anti-Virus products that provide both anti-virus and anti-spyware functionality are also listed in the Anti-spyware products list

Require any supported product.

Require specific products/vendors

Require any supported product from a specific vendor.

Require specific products

▼ Optional

Monitor this rule for change in result

Note: Enabling this option will report change in compliance for this rule to the Pulse Policy Secure immediately. The client component requires additional computing cycles to report change in compliance immediately. We strongly recommend that this option be enabled for rules that are dynamic in nature, for example a rule for RTP check provided by AntiVirus software. For other rules the host checker update frequency should be used to get periodic health checks from endpoints.

Powered by
OPSWAT

5. Enter a name for the firewall rule.
6. Select one of the following options:
 - **Require any supported product** allows you to check for any product (rather than requiring you to select every product separately). This option button provides a list of products in the remediation section to allow you to enable remediation options which are product specific.
 - **Require specific products/vendors** allows you to define compliance by allowing any product by a specific vendor or provides functionality that allows you to select individual products to define compliance.
7. Under Optional, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, IPS initiates a new handshake to re-evaluate realm or role assignments.
8. Click **Save Changes**.

- Under Rule Settings, select **Predefined: HardDisk Encryption** and then click **Add**.

rule (Predefined Rule : HardDisk Encryption)

Rule Type: HardDisk Encryption

*Rule Name:

▼ *Criteria

Require any supported product.

Require specific products/vendors

Drive Configuration Details:

All Drives

Specific Drives

Drive Letters: Example: To check encryption status of C, D and E drives, configure "C,D,E"

Consider policy as passed if the drives are not detected.

Note: Enabling this option will result in policy pass if any of the configured drives are not detected on the endpoint machine.

Consider policy as passed if the drive Encryption is in progress.

Note: Enabling this option will result in policy pass if any of the configured drives are not fully encrypted, but the encryption process is in progress on the endpoint machine.

Powered by
OPSWAT

* indicates required field

- Enter a Rule Name for the HardDisk Encryption rule.
- Select one of the following options:
 - Require any supported product** allows you to check for any product (rather than requiring you to select every product separately). This option button provides a list of products in the remediation section to allow you to enable remediation options which are product specific.
 - Require specific products/vendors** allows you to define compliance by allowing any product by a specific vendor or provides functionality that allows you to select individual products to define compliance.

8. Under Drive Configuration, select the required option.
 - All Drives--(Default) Select this option to check if all the drives on the client machine are encrypted.
 - **Specific Drives**-Select this option to check if only specific drives on the client machine are encrypted.
 - **Drive Letters**– Enter the drive name. For example, C, D, E.
 - **Consider policy as passed if the drives are not detected**– Select this option to consider policy as passed if the drives are not detected
 - **Consider policy as passed if the drive Encryption is in progress**– Select this option to allow the Host Checker policy to pass if the encryption process is in progress and the drive is not fully encrypted. The drive encryption process takes time to complete depending up on the drive size and contents. For multiple drives, the HC policy passes only if the encryption process is in progress in all the drives.
9. Click **Save Changes**.

Configuring Common Vulnerability and Exposure (CVE) Check Rules

Host Checker is used for analyzing the health of the endpoint before providing access to the network. As endpoints are vulnerable to many types of new attacks such as Ransomware attack. It becomes extremely important to identify such endpoints, which are vulnerable to any attacks. The CVE lists some of these attacks along with the required software patches to prevent from such attacks. IPS provides the CVE check rule, which helps in identifying the endpoints which are vulnerable using the OPSWAT library. If the endpoint is vulnerable appropriate action is taken based on the rule configuration. For example, the user can be denied from accessing the network.



- CVE check rule is supported from ESAP 3.2.3 onwards.
- OPSWAT version 3 does not support CVE rules. These rules will always be evaluated as failed and may cause the host checker policy to fail. It is recommended to delete CVE rules if you are using OPSWAT V3 SDK for evaluation.

To configure a predefined CVE check rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy, or click an existing policy in the Policies section of the page.

- Click the **Windows** tab.
- Under Rule Settings, select **Predefined: CVE Checks** and click **Add**.

Endpoint Security > Host Checker Policy

Host Checker Policy

Use this restriction to limit this policy to users whose workstations are running host-checking software.

Policy Name:

Windows Mac Linux Solaris

▼ Rule Settings

- Select Rule Type -

Search:

Rule Type	Summary
- Select Rule Type -	
Predefined: Antivirus	
Predefined: Firewall	
Predefined: AntiSpyware	
Predefined: HardDisk Encryption	
Predefined: Patch Management	
Predefined: OS Checks	
Predefined: CVE Checks	
Custom: 3rd Party NHC Check	
Custom: Ports	
Custom: Process	
Custom: File	
Custom: Registry Setting	
Custom: NetBIOS	
Custom: MAC Address	
Custom: Machine Certificate	
Custom: Advanced Host Checking	
Custom: Statement of Health	

Enable Custom Instructions
 Kill Processes
 Delete Files
 Send reason strings

▼ Dashboard Reporting

Consider for Dashboard/Reporting

Note: If this checkbox is not selected, policy details are not reported to dashboard. In other words, even if this policy fails, the endpoint compliance state is not affected in dashboard charts and reports.

- Enter a Rule Name for the CVE Check rule. For example, you can configure a check for WannaCry vulnerability.

Configuration > Host Checker Policy > Add Predefined Rule : CVE Checks

Add Predefined Rule : CVE Checks

Rule Type: CVE Checks

*Rule Name:

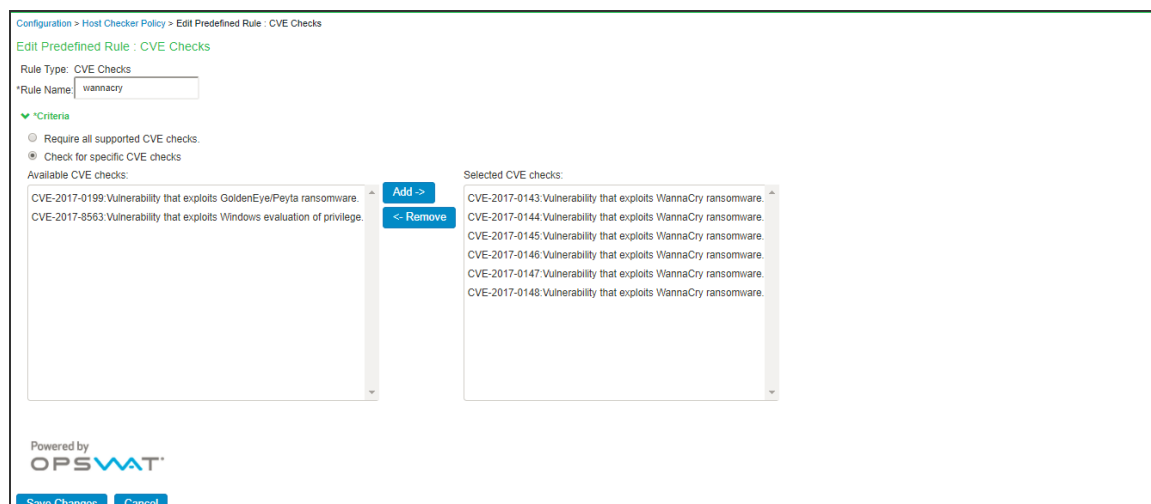
▼ *Criteria

Require all supported CVE checks.
 Check for specific CVE checks

Powered by
OPSWAT

* indicates required field

- From the Criteria, select if you require all the CVE checks from OPSWAT or choose the specific CVE checks from the available CVE checks list.



- Click **Save Changes**.

Configuring Patch Management Rules

You can configure Host Checker to check for installed Patch Management Software on endpoints.

Patch management software detects patch status based on the configured rules on corresponding patch management server. Detection of patches status on the client machine depends on the support provided by the 3rd party patch management solution that is used. Hence different patch management software on the same client can report the status differently. To avoid conflicts, administrator is allowed to configure only one patch management software product on policy configuration page.

It provides options to configure various Severity and Category options that administrator is interested in. These additional details are used during policy evaluation such that only the missing patches that belongs to configured "Severity" and "Category" are considered. Any other patches that does not belong to configured "Severity" and "Category" are not considered during policy evaluation.

The default "Severity" options selected in policy are Critical, Important. The default "Category" options selected in policy are Security Update, Critical Update, Regular Update, Driver Update.



- The remediation support for patch management rule is available only for Windows platform using SCCM client.
- Patch Management on Mac is not supported with OPSWAT SDK V3 and pre-9.0R1 Pulse clients.

To configure a predefined patch management rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy, or click an existing policy in the Policies section of the page.
3. Click the **Windows/Mac** tab.
4. Enter a Rule Name for the Patch Management rule.

Endpoint Security > Host Checker Policy

Host Checker Policy

Use this restriction to limit this policy to users whose workstations are running host-checking software.

Policy Name: HC_Patch

Windows **Mac** Linux Solaris

▼ Rule Settings

- Select Rule Type - Add Delete

Predefined: Antivirus
Predefined: Firewall
Predefined: AntiSpyware
Predefined: HardDisk Encryption
Predefined: Patch Management
Custom: Ports
Custom: Process
Custom: File
Custom: Machine Certificate

Search:

Rule Type	Summary

← Previous 1 Next →

All of the above rules
 Any of the above rules
 Custom...

5. Under Rule Settings, select **Predefined: Patch Management** and click **Add**.
6. From the Criteria, select the **Patch Management Software** to be installed on the endpoint.
7. Select the **Severity** and **Category** details of the patches to be evaluated.



For patch management products that do not provide "Severity" and "Category" details, administrator can choose the "Unknown" options so that all the reported missing patches are considered in policy evaluation.

8. (Windows Only) If you want to do remediation, Under the Remediation section, select **Enable Automatic Patch Deployment**.
9. Click **Save Changes**.

Configuration > Host Checker Policy > Add Predefined Rule : Patch Management

Add Predefined Rule : Patch Management

Rule Type: Patch Management

*Rule Name:

▼ *Criteria

Select Product Name:

Severity: Critical Important Moderate Low Unspecified/Unknown

Note: For some of the patch management software products, severity is not detected. In such cases, enable "Unspecified/Unknown" severity to detect the missing patches

Category: Security Update Rollup Update Critical Update Regular Update Driver Update Service Pack Update Unknown

Note: For some of the patch management software products, category is not detected. In such cases, enable "Unknown" category to detect the missing patches

Powered by
OPSWAT

* indicates required field

Configuring OS Checks Rule

You can configure Host Checker to check for the Windows/MAC operating systems and minimum service pack versions that you specify. Any service pack whose version is greater than or equal to the version you specify satisfies the policy.



OS Check rule is supported starting from MAC OS X El Captain (10.11) and above.

To configure a rule for OS checks:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy, or click an existing policy in the Policies section of the page.
3. Click the **Windows/Mac** tab.
4. Enter a Rule Name for the OS checks rule.

- Under Rule Settings, select **Predefined: OS checks** and click **Add**.

Configuration > Host Checker Policy > Add Predefined Rule - OS Checks

Add Predefined Rule : OS Checks

Rule Type: OS Checks

*Rule Name:

▼ *Criteria

- Windows 10
Minimum Service Pack/Version:
- Windows 10 64-Bit
Minimum Service Pack/Version:
- Windows 2000
Minimum Service Pack/Version:
- Windows 2003
Minimum Service Pack/Version:
- Windows 2003 64-Bit
Minimum Service Pack/Version:
- Windows 2008
Minimum Service Pack/Version:
- Windows 2008 R2 64-Bit
Minimum Service Pack/Version:
- Windows 7
Minimum Service Pack/Version:
- Windows 7 64-Bit
Minimum Service Pack/Version:
- Windows 8
Minimum Service Pack/Version:
- Windows 8 64-Bit
Minimum Service Pack/Version:
- Windows 8.1
Minimum Service Pack/Version:
- Windows 8.1 64-Bit
Minimum Service Pack/Version:
- Windows Universal-App
Minimum Service Pack/Version:
- Windows Universal-App 64-Bit
Minimum Service Pack/Version:
- Windows Universal-App-ARM
Minimum Service Pack/Version:
- Windows VPN-Plugin
Minimum Service Pack/Version:
- Windows VPN-Plugin 64-Bit
Minimum Service Pack/Version:
- Windows VPN-Plugin-ARM
Minimum Service Pack/Version:
- Windows Vista
Minimum Service Pack/Version:
- Windows Vista 64-Bit
Minimum Service Pack/Version:
- Windows XP
Minimum Service Pack/Version:
- Windows XP 64-Bit
Minimum Service Pack/Version:

* indicates required field

Configuration > Host Checker Policy > Add Predefined Rule - OS Checks

Add Predefined Rule : OS Checks

Rule Type: OS Checks

*Rule Name:

▼ *Criteria

- Mac El-Capitan
Minimum Service Pack/Version:
- Mac High-Sierra
Minimum Service Pack/Version:
- Mac Sierra
Minimum Service Pack/Version:

* indicates required field

- From the Criteria, select the **Windows/Mac operating systems** and minimum service pack/version to be there on the endpoint.
- Click **Save Changes**.

Configuring Third-Party NHC Rule

Use this rule type to specify the location of a custom DLL. Host Checker calls the DLL to perform customized client-side checks.

To configure a rule for third-party NHC:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Under Rule Settings, select **Custom: 3rd Party NHC Check** and then click **Add**.

3. Enter a name for the NHC Check rule.
4. Under Criteria, enter the Vendor name and Path to NHC DLL.
5. Under Optional, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, the IPS initiates a new handshake to re-evaluate realm or role assignments.
6. Click **Save Changes**.

Configuring Ports Rule

Use this rule type to control the network connections that a client can generate during a session. This rule type ensures that certain ports are open or closed on the client machine before the user can access the system.

To configure a custom port rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy, or click an existing policy in the Policies section of the page.

- Under Rule Settings, select **Custom: ports** and then click **Add**.

Configuration > Host Checker Policy > Add Custom Rule : Ports

Add Custom Rule : Ports

Rule Type: Ports

*Rule Name:

▼ *Criteria

*Port List: Enter port numbers separated by comma

Required Deny

▼ Optional

Monitor this rule for change in result

Note: Enabling this option will report change in compliance for this rule to the Pulse Policy Secure immediately. The client component requires additional computing cycles to report change in compliance immediately. We strongly recommend that this option be enabled for rules that are dynamic in nature, for example a rule for RTP check provided by AntiVirus software. For other rules the host checker update frequency should be used to get periodic health checks from endpoints.

* indicates required field

- Enter a name for the port rule.
- Under Criteria, enter a comma delimited list (without spaces) of ports or port ranges, such as: 1234,11000- 11999,1235. Select Required if you want these ports to be open on the client machine or Deny if you want them to be closed.
- (Windows only) Under Optional, select Monitor this rule for change in result to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, the IPS initiates a new handshake to re-evaluate realm or role assignments.
- Click **Save changes**.

Configuring Process Rule

Use this rule type to control the software that a client may run during a session. This rule type ensures that certain processes are running or not running on the client machine before the user can access protected resources.

To configure a custom process rule:

- Select **Authentication > Endpoint Security > Host Checker**.
- Create a new policy, or click an existing policy in the Policies section of the page.

- Under Rule Settings, select Custom: **Process** and then click **Add**.

Configuration > Host Checker Policy > Add Custom Rule : Process

Add Custom Rule : Process

Rule Type: Process

*Rule Name:

▼ *Criteria

*Process Name:

Required Deny

▼ Optional

MD5 Checksums: One MD5 checksum per line.

SHA256 Checksums: One SHA256 checksum per line.

Monitor this rule for change in result

Note: Enabling this option will report change in compliance for this rule to the Pulse Policy Secure immediately. The client component requires additional computing cycles to report change nature , for example a rule for RTP check provided by AntiVirus software. For other rules the host checker update frequency should be used to get periodic health checks from endpoints.

* indicates required field

- Enter a name for the process rule.
- Under Criteria, enter the name of a process (executable file), such as: good-app.exe. You can use a wildcard character to specify the process name. For example: good*.exe. Select Required to require that this process is running or Deny to require that this process is not running.

6. Under **Optional**, enable the checks required from the following:
 - Specify the MD5 checksum value of each executable file to which you want the policy to apply. For example, an executable may have different MD5 checksum values on a desktop, laptop, or different operating systems. On a system with OpenSSL installed—Macintosh, Linux and Solaris systems have OpenSSL installed by default—you can determine the MD5 checksum by using this command: `openssl md5 <processFilePath>`.
 - Specify the SHA256 checksum value of each file.
 - Select or clear the check box next to **Monitor this rule for change in result**. With the checkbox enabled, it continuously monitors the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, the IPS initiates a new handshake to re-evaluate realm or role assignments.
7. Click **Save Changes**.

Configuring File Rule

Use this rule type to ensure that certain files are present or not present on the client machine before the user can access. You may also use file checks to evaluate the age and content (through MD5 checksums) of required files and allow or deny access accordingly.

To configure a custom file rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy, or click an existing policy in the **Policies** section of the page.
3. Under **Rule Settings**, select **Custom: File** and then click **Add**.

4. Enter a name for the file rule.

Configuration > Host Checker Policy > Add Custom Rule : File

Add Custom Rule : File

Rule Type: File

*Rule Name:

▼ *Criteria

*File Name: Example: c:\temp\bad-file.txt or <%windir%>\bad-file.txt

Required Deny

▼ Optional

Minimum version:

File modified less than: days ago.

MD5 Checksums: One MD5 checksum per line.

SHA256 Checksums: One SHA256 checksum per line.

Monitor this rule for change in result

Note: Enabling this option will report change in compliance for this rule to the Pulse Policy Secure immediately. The client component requires additional computing cycles to report change nature, for example a rule for RTP check provided by AntiVirus software. For other rules the host checker update frequency should be used to get periodic health checks from endpoints.

* indicates required field

5. Under Criteria, enter the name of a file (any file type), For example, **c:\temp\bad-file.txt** or **/temp/bad-file.txt**. You can use a wildcard character to specify the file name. For example: *.txt. You can also use an environment variable to specify the directory path to the file. (You cannot use a wildcard character in the directory path.) Enclose the variable between the <% and %> characters. For example: <%windir%>\bad-file.txt
6. Select Required to require that this file is present on the client machine or Deny to require that this file is not present.

7. (Windows only) Under Optional, enable the checks required from the following:
 - Specify the minimum version of the file (optional). For example, if you require notepad.exe to be present on the client, you can enter 5.0 in the field. Host Checker accepts version 5.0 and above, of notepad.exe.
 - Specify the maximum age (File modified less than n days) (in days) for a file (optional). If the file is older than the specified number of days, then the client does not meet the attribute check requirement.
 - Specify the MD5 checksum value of each file to which you want the policy to apply (optional). On Macintosh, Linux and Solaris, you can determine the MD5 checksum by using this command: **openssl md5 <filePath>**
8. Specify the SHA256 checksum value of each file.
9. Select Monitor this rule for change in result to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, the IPS initiates a new handshake to re-evaluate realm or role assignments.
10. Click **Save Changes**.

Configuring Registry Settings Rule

Use this rule type to control the corporate PC images, system configurations, and software settings that a client must have to access the IPS. This rule type ensures that certain registry keys are set on the client machine before the user can access the IPS. You may also use registry checks to evaluate the age of required files and to allow or deny access accordingly.

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy, or click an existing policy in the Policies section of the page.

- Under Rule Settings, select **Custom: Registry Setting** and then click **Add**.

The screenshot shows the 'Add Custom Rule: Registry Setting' configuration window. The breadcrumb path is 'Configuration > Host Checker Policy > Add Custom Rule: Registry Setting'. The 'Rule Type' is 'Registry Setting'. The 'Rule Name' field is empty. Under the 'Criteria' section, the 'Registry Root key' is set to 'HKEY_LOCAL_MACHINE'. The 'Registry Subkey', 'Name', and 'Value' fields are empty. The 'Type' is set to 'String'. There are two checkboxes: 'Check for 64-bit registry' (unchecked) and 'Minimum version' (checked). A note states: 'Note: Check for 64 bit registry. This option is applicable only for 64-bit versions of Windows. By default, Host Checker checks only 32-bit registry.' Under the 'Optional' section, the checkbox 'Monitor this rule for change in result' is unchecked. A note explains: 'Note: Enabling this option will report change in compliance for this rule to the Pulse Policy Secure immediately. The client component requires additional computing cycles to report change in compliance immediately. We strongly recommend that this option be enabled for rules that are dynamic in nature, for example a rule for RTP check provided by Antivirus software. For other rules the host checker update frequency should be used to get periodic health checks from endpoints.' Under the 'Remediation' section, the checkbox 'Set Registry value specified in criteria' is unchecked.

- Enter a name for the registry setting rule.
- Under the criteria:
 - Select a root key from the drop-down list.
 - Enter the path to the application folder for the registry subkey.
 - Enter the name of the key's value that you want to require (optional). This name appears in the **Name** column of the Registry Editor.
 - Select the key value's type (**String, Binary, or DWORD**) from the drop-down list (optional). This type appears in the Type column of the Registry Editor.
 - Specify the required registry key value (optional). This information appears in the Data column of the Registry Editor.
 - If the key value represents an application version, select **Minimum version** to allow the specified version or newer.
- Under Optional, select **Monitor this rule for change in result to continuously monitor the policy compliance of endpoints**. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, the system initiates a new handshake to re-evaluate realm or role assignments.
- Under Remediation, Select the check box for **Set Registry value** specified in criteria.
- Click **Save Changes**.

Configuring NetBIOS Rule

Use this rule type to check the NetBIOS name of the client machine before the user can access IPS.



A maximum of 1,000 regex patterns are supported in a single NetBIOS rule. In case, if there are more than 1,000 regex patterns in a single rule, split the rule into multiple rules.

To configure a custom NetBIOS rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy, or click an existing policy in the Policies section of the page.
3. Under Rule Settings, select **Custom: File** and then click **Add**.

4. Enter a name for the NetBIOS rule.

Configuration > Host Checker Policy > Add Custom Rule : NetBIOS

Add Custom Rule : NetBIOS

Rule Type: NetBIOS

*Rule Name:

▼ *Criteria

*NetBIOS Names: One per line
Example: WINDOWS-PC,WIN*-PC,*-PC,WINDOWS*

Required Deny

* indicates required field

Configuration > Host Checker Policy > Add Custom Rule : NetBIOS

Add Custom Rule : NetBIOS

Rule Type: NetBIOS

*Rule Name:

▼ *Criteria

*NetBIOS Names: One per line
Example: MACBOOK-PRO,MAC*-PRO,*-PRO,MACBOOK*

Required Deny

* indicates required field

- Under Criteria, enter a comma-delimited list (without spaces) of NetBIOS names. The name can be up to 15 characters in length. You can use wildcard characters in the name and it is not case-sensitive. For example, md*, m*xp and *xp all match MDXP. Select Required to require that this file is present on the client machine or Deny to require that this file is not present.



For Mac OS, you can enter special characters "[!\"#\$%&'()*+,-./:;<=>?@\[\]\^_`{|}~]" and space is allowed between NetBIOS names.

- Select Required to require that NETBIOS name of the client machine match one of the names you specify, or Deny to require that the name does not match any name.
- Click **Save Changes**.

Configuring MAC Address Rule

Use this rule type to check the MAC addresses of the client machine before the user can access the IPS.

To configure a custom MAC Address Rule:

- Select **Authentication > Endpoint Security > Host Checker**.
- Create a new policy or click an existing policy in the Policies section of the page.
- Under Rule Settings, select **Custom: MAC Address** and then click **Add**.
- Enter a name for the MAC address rule.

Configuration > Host Checker Policy > Add Custom Rule : MAC Address

Add Custom Rule : MAC Address

Rule Type: MAC Address

*Rule Name:

▼ *Criteria

*MAC Addresses: Example
00:11:85:bb:8c:*
00:ff:*:*:*
One per line

Required Deny

* indicates required field

5. Under **Criteria**, enter a comma-delimited list (without spaces) of MAC addresses in the form XX:XX:XX:XX:XX:XX where the X's are hexadecimal numbers. For example: 00:0e:1b:04:40:29. You can use a * wildcard character to represent a two-character section of the address. For example, you can use a * to represent the "04", "40", and "29" sections of the previous example address: 00:0e:1b:*:* But you cannot use a * to represent a single character. For example, the * in the following address is not allowed: 00:0e:1b:04:40:*9
6. Select **Required** to require that a MAC address of the client machine matches any of the addresses you specify, or **Deny** to require that the all addresses do not match. A client machine will have at least one MAC address for each network connection, such as Ethernet, wireless, and VPN.
7. This rule's requirement is met if there is a match between any of the addresses you specify and any MAC address on the client machine.
8. Click **Save Changes**.

Configuring Machine Certificate Rule

Use this rule type to check that the client machine is permitted access by validating the machine certificate stored on the client machine.

To configure a machine certificate rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy, or click an existing policy in the **Policies** section of the page.
3. Under **Rule Settings**, select **Custom: Machine certificate** and then click **Add**.

- Enter a name for the machine certificate rule.

Configuration > Host Checker Policy > Add Custom Rule : Machine Certificate

Add Custom Rule : Machine Certificate

Rule Type: Machine Certificate

*Rule Name:

▼ *Criteria

Select Issuer Certificate: Any Certificate

▼ Optional

You can optionally require specific values in the machine certificate:

Certificate field (example "cn")	Expected value	
<input type="text"/>	<input type="text"/>	Add
<input type="text"/>	<input type="text"/>	

Edit Delete

Save Changes Cancel

* indicates required field

- Under Criteria, Select Issuer Certificate list, select the certificate that you want to retrieve from the user's machine and validate. Or, select **Any Certificate** to skip the issuer check and only validate the machine certificate based on the optional criteria that you specify below.
- From the Optional fields (**Certificate field and Expected value**), specify any additional criteria that Host Checker should use when verifying the machine certificate.

- If more than one certificate is installed on the client machine that matches the specified criteria, The Host Checker client passes the first certificate it finds to IPS for validation.



- Admin must perform some additional configurations on the Client machine for installing machine certificate on MAC OS due to some restrictions from Apple. For more information, see [KB44148](#)

- Click **Save Changes**.

Configuring Advanced Host Checking Rule

Use this rule type to combine multiple policies for performing advanced host checking. The supported policy types are ports, process, file, registry setting, NETBIOS, MAC address and machine certificate. It allows Administrator to dynamically configure the expected values from registry locations on the endpoint for evaluating the policies.



This feature is supported only on Windows platform.

To configure an advanced host checking rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy, or click an existing policy in the Policies section of the page.
3. Under Rule Settings, select **Custom: Advanced Host Checking** and then click **Add**.
4. Enter a name for the rule.
5. Select the check to be performed from the Rule Type list.

Configuration > Host Checker Policy > Add Custom Rule : Advanced Host Checking

Add Custom Rule : Advanced Host Checking

Rule Type: Advanced Host Checking

*Rule Name:

▼ *Criteria

*Select Check Type: Select the check to be performed
 Required Deny

*Method to obtain value: Registry Setting

Registry Root key:

Registry Subkey:

Name:

Type:
 Check for 64-bit registry

Note: Check for 64 bit registry. This option is applicable only for 64-bit versions of Windows. By default, Host Checker checks only 32-bit registry.

* indicates required field

6. Under Criteria, **Select Rule Type** list.

- Select Ports to check whether a specific port number is opened or closed on the endpoint.
 - Enable **Required/Deny** to check if the specified port is open/closed.
 - Select the registry root key- HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG, or HKEY_CLASSES_ROOT.
 - Enter the registry subkey.
 - Enter the name of the registry.
 - Select the type of the registry- String, Binary, or DWORD.
 - Select **Check for 64-bit registry** to check the 64 bit registry on Windows. The default is 32 bit registry.



You can similarly add the check type for Process/File/NETBIOS/MAC Address. The port number/process name/file path/NETBIOS name/MAC address is obtained from the Registry setting.

Configuration > Host Checker Policy > Add Custom Rule : Advanced Host Checking

Add Custom Rule : Advanced Host Checking

Rule Type: Advanced Host Checking

*Rule Name:

▼ *Criteria

*Select Check Type: Select the check to be performed

Required Deny

*Method to obtain Ports value

Registry Root key:

Registry Subkey:

Name:

Type:

Check for 64-bit registry

Note: Check for 64 bit registry. This option is applicable only for 64-bit versions of Windows. By default, Host Checker checks only 32-bit registry.

- Select **Registry Setting** to verify the specific registry values on the endpoint. You can define only the registry location in the policy and define another registry location, which provides the expected registry value.
 - Select the registry root key- HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG, or HKEY_CLASSES_ROOT.
 - Enter the registry subkey.
 - Enter the name.
 - Select the type of the registry- String, Binary, or DWORD.
 - Configure another registry setting to fetch the expected registry value. Select the registry subkey, name, and type.

The screenshot shows the 'Add Custom Rule' configuration window for 'Advanced Host Checking'. The window is titled 'Configuration > Host Checker Policy > Add Custom Rule : Advanced Host Checking'. Below the title, it says 'Add Custom Rule : Advanced Host Checking'. The 'Rule Type' is set to 'Advanced Host Checking'. There is a text input field for '*Rule Name:'. Under the '*Criteria' section, there are two identical configuration blocks. The first block is for '*Select Check Type:' and the second is for '*Method to obtain Registry Setting value'. Both blocks have a 'Registry Root key:' dropdown set to 'HKEY_LOCAL_MACHINE', a 'Registry Subkey:' text input, a 'Name:' text input, and a 'Type:' dropdown set to 'String'. There is a checkbox for 'Check for 64-bit registry' which is currently unchecked. A note below each block states: 'Note: Check for 64 bit registry. This option is applicable only for 64-bit versions of Windows. By default, Host Checker checks only 32-bit registry.' At the bottom of the window, there are 'Save Changes' and 'Cancel' buttons.

- Select **Machine Certificate** to verify the required certificate is installed on the client machine certificate store.
- Select the issuer certificate from the list.

- Specify any additional criteria that Host Checker must use while verifying the certificate.
 - Enter the certificate field name. For example, cn.
 - Select the registry key.
 - Enter the registry subkey.
 - Enter the registry name.
 - Select the registry type.
- Click **Add**.

The screenshot shows the 'Add Custom Rule' configuration page for 'Advanced Host Checking'. The page includes a breadcrumb trail: Configuration > Host Checker Policy > Add Custom Rule > Advanced Host Checking. The rule type is set to 'Advanced Host Checking'. There is a text input field for the 'Rule Name'. Under the 'Criteria' section, there are two dropdown menus: '*Select Check Type:' set to 'Machine Certificate' and '*Select Issuer Certificate:' set to 'Any Certificate'. An 'Optional' section contains a note: 'You can optionally require specific values in the machine certificate:'. Below this is a table with columns: Certificate field (example "cn"), Registry Key, Registry SubKey, Registry Name, Registry Type, and Registry 64bit. The 'Registry Key' dropdown is set to 'HKEY_LOCAL_MACHINE'. The 'Registry Type' dropdown is set to 'String'. There is a checkbox for 'Registry 64bit' which is currently unchecked. An 'Add' button is at the end of the table row. Below the table are 'Edit' and 'Delete' buttons. At the bottom of the form are 'Save Changes' and 'Cancel' buttons.

Certificate field (example "cn")	Registry Key	Registry SubKey	Registry Name	Registry Type	Registry 64bit
<input type="text"/>	HKEY_LOCAL_MACHINE	<input type="text"/>	<input type="text"/>	String	<input type="checkbox"/>

7. Click **Save Changes**.

Configuring Statement of Health Rule

Use this rule type to evaluate endpoint's health status and make policy decisions for network access based on the result.

To configure a custom state of health rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy, or click an existing policy in the Policies section of the page.
3. For a new policy, specify a name for the policy and then click Continue.

- Under Rule Settings, select **Custom: Statement of Health** and then click **Add**.

Configuration > Host Checker Policy > Add Custom Rule : Statement of Health

Add Custom Rule : Statement of Health

Rule Type: Statement of Health

*Rule Name:

▼ *Criteria

- Antivirus Enabled
- Antivirus up to date
- Antispyware enabled
- Antispyware up to date
- Firewall Enabled
- Automatic Updates Enabled

* indicates required field

- Enter a Name for the SOH rule.
- Under Criteria, enter a Label for a SOH parameter. Select an SOH policy option from the Parameter menu then click **Add** for the following types:
 - Antivirus Enabled
 - Antivirus up to date
 - Antispyware enabled
 - Antispyware up to date
 - Firewall Enabled
 - Automatic Updates Enabled
- Select additional options from the Parameter list to add additional SOH parameters.

- (Optional) For each rule, select the Enable automatic remediation check box. If you select this option for a rule, the user receives a remediation message from the SoH agent, and appropriate remediation is performed, if possible. If the box is not selected, the user receives a remediation message, but no remediation action is performed.
- Click **Save Changes**.

Configuring System Integrity Protection Rule

System Integrity Protection (SIP) is a security feature introduced in Mac OS X El Capitan. This security feature from Apple provides security on the endpoint machine by restricting various actions that root user can perform on the client machine. System Integrity Protection is enabled by default but can be disabled.

IPS supports System Integrity Protection policy to check the status of System Integrity Protection (SIP) on the Mac OS endpoints. Using this, the administrators can provide different access level to the endpoints based on the status of "System Integrity Protection" on the client machines.

To configure a Host Checker Predefined SIP rule:

- Select **Authentication > Endpoint Security > Host Checker**.
- Create a new or click an existing policy in the Policies section of the page.
- Select the tab for **Mac**.
- Under Rule Settings, select **Predefined: System Integrity Protection Rule** and click **Add**.

The screenshot shows the configuration page for adding a predefined rule. The breadcrumb is "Configuration > Host Checker Policy > Add Predefined Rule : System Integrity Protection". The title is "Add Predefined Rule : System Integrity Protection". The "Rule Type" is "System Integrity Protection". The "Rule Name" field contains "SIP". Under the "Criteria" section, the text reads "Ensure status of System Integrity Protection on client machine is in below state" with radio buttons for "Enabled" (selected) and "Disabled". A note states: "Note: Status of System Integrity Protection on client machine is considered as disabled in case client machine (prior to El Capitan) does not have support for System Integrity Protection". At the bottom are "Save Changes" and "Cancel" buttons. A footnote indicates "* indicates required field".

- Enter the rule name.

6. Under Criteria, select **Enabled** to ensure that the System Integrity Protection on the client machine is enabled.
7. Click **Save Changes**.

Configuring Command Rule

Command Rule enables administrators to check the versions of the installed applications on the Mac OS endpoints.

To configure a Host Checker: Custom command rule:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create a new or click an existing policy in the Policies section of the page.
3. Select the tab for Mac.
4. Under Rule Settings, select **Custom: Command** and click **Add**.

Configuration > Host Checker Policy > Add Command

Add Command

Rule Type: Command

*Rule Name:

▼ *Criteria

* Command: ▼

* Property list file: Note: Path of the Property list file on the client machine. Ex: /Applications/Utilities/Terminal.app/Contents/Info.plist

* Key in Property list file: Note: Key name in above Property list file. Ex: CFBundleShortVersionString

* Expected Value(s): Note: Multiple values can be provided by using comma as separator. Ex: 2000, 2001. Wildcard is supported in the expected value. Ex: 2*

* indicates required field

5. Enter the rule name.
6. Under Criteria, complete the following configuration:
 - Select the command type as **default read (Read Settings)**.
 - Specify the path of the property list file of the required application on the client machine.
 - Enter the key name used in the property list file for obtaining the version of the application.
 - Enter the expected version that needs to be present on the client machine.

7. Click **Save Changes**.



Ensure that the required ESAP package (which has support for Command Rule) is installed and activated on the server.

Using a Wildcard or Environment Variable in a Host Checker Rule

The following table lists the wildcards you can use to specify a file name in a File rule or a process name in a Process rule.

Wildcard Character	Description	Example
*	Matches any character	*.txt
?	Matches exactly one character	app-?.exe

In a **Custom File rule** for Windows, you can use the following environment variables to specify the directory path to a file:

Environment variable	Example Windows Value
<%APPDATA%>	C:\Documents and Settings\jdoe\Application Data
<%windir%>	C:\WINDOWS
<%ProgramFiles%>	C:\Program Files
<%CommonProgramFiles%>	C:\Program Files\Common Files
<%USERPROFILE%>	C:\Documents and Settings\jdoe
<%HOMEDRIVE%>	C:
<%Temp%>	C:\Documents and Settings \<username>\Local Settings\Temp

The following table lists File rules for Macintosh, Linux and Solaris.

Environment variable	Example Macintosh Value	Example Linux and Solaris Values
<%Java.home%>	/System/Library/Frameworks/JavaVM.framework/Versions/1.4.2/Home	/local/local/Java/j2sdk1.4.1_02/jre
<%Java.io.tmpdir%>	/tmp	/tmp
<%user.dir%>	/Users/admin	/home-shared/cknouse
<%user.home%>	/Users/admin	/home/cknouse

Configuring Third-Party Integrity Measurement Verifiers (IMV)

The TNC standard enables the enforcement of security requirements for endpoints connecting to networks. You can configure Host Checker to monitor third-party TNC-compliant IMCs installed on client computers. To do so, you must:

1. Run the Third-party Integrity Measurement Verifier (IMV) Server installer on the system designated as the remote IMV server. Install the third-party IMVs and create the server certificates. You can download this installer from Maintenance > system > Installers.
2. Specify the remote IMV server so that IPS can communicate with it.
3. Implement the Host Checker policy. Once you configure the remote IMV server, IPS adds the policy type Custom: remote IMV.

Configuring a Remote IMV Server

The third-party IMVs are installed on the remote IMV server and not on IPS and then obtain a server certificate for the remote IMV server. Import the trusted root CA certificate of the CA that generated the server certificate to IPS. IPS then authenticates with the remote IMV server through the certificate. If you do not have a CA, install and use OpenSSL to generate a CA certificate.

To configure the remote IMV server:

1. Select **Maintenance > System > Installers** and download the third-party Measurement Verifier (IMV) server installer.
2. Run the installer on the system designated as the remote IMV server.
3. Install the third-party IMVs on the remote IMV server and the corresponding IMCs on the client systems.
4. Generate a server certificate from a certificate authority for the remote IMV server. The server's certificate Subject CN value must contain the actual host name or IP address of the remote IMV server.

The server certificate and the private key must be combined into a single PKCS#12 file and must be encrypted with a password. If you do not have a CA, you can use OpenSSL to create one, and then create a server certificate for the remote IMV server.

Configuring a Third-Party IMV Policy

To use Host Checker as a policy enforcement tool for managing endpoints, you must create global Host Checker policies at the system level and then implement the policies at the realm and role levels.



The Custom: Remote IMV option does not appear until you add the Remote IMV New Server and New IMV on the main Host Checker page.

To configure a third-party IMV policy:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Under Policies, click **New**.
3. Enter a name in the Policy Name field and click **Continue**. (Users see this name on the Host Checker remediation page if you enable custom instructions for this policy.)
4. Under Rule Settings, select Custom: Remote IMV and click **Add**.
5. In the Add Custom Rule: Remote IMV page:
 - In the **Rule Name** field, enter an identifier for the rule.
 - Under Criteria, select the **third-party IMV** to associate with this rule.
6. Click **Save Changes**.

7. Specify how Host Checker must evaluate multiple rules within the policy.
8. (Recommended) Specify remediation options for users whose computers do not meet the requirements specified in the policy.
9. Click **Save Changes**.
10. Implement the policy at the realm or role level.

Configuring General Host Checker Remediation

To specify remediation actions for a Host Checker policy:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Create or enable Host Checker policies.

- Specify the remediation actions for Host Checker to perform if a computer does not meet the requirements of the current policy:
 - Enable Custom Instructions**—Enter the instructions to display to the user on the Host Checker remediation page. You can use the following HTML tags to format text and to add links to resources such as policy servers or web sites: `<i>`, ``, `
`, ``, and `<a href>`. For example:

```
You do not have the latest signature files.  
<a href="www.company.com">Click here to download the latest signature files.</a>
```
 - Kill Processes**—On each line, enter the name of one or more processes to kill if the computer does not meet the policy requirements. You can include an optional MD5 checksum for the process. (You cannot use wildcards in the process name.) For example:

```
keylogger.exe  
MD5: 6A7DFAF12C3183B56C44E89B12DBEF56
```
 - Delete Files**—Enter the names of files to delete if the user's computer does not meet the policy requirements. (You cannot use wildcards in the file name.) Enter one filename per line. For example:

```
c:\temp\bad-file.txt  
/temp/bad-file.txt
```
 - Send reason strings**—Select this option to display a message to users (called a reason string) that is returned by Host Checker or IMV and that explains why the client machine does not meet the Host Checker policy requirements. This option applies to predefined rules, to custom rules, and to third-party IMVs that use extensions in the Ivanti TNC SDK. For example, an antivirus IMV might display the following reason string:

The AntiVirus Product Version is too low. The age of the Virus Definitions is not acceptable.

- Click **Save Changes**.

Store and Reuse Host Checker Policy Results

The Host Checker configuration page enables you to store and reuse the host checker evaluation results. The admin can configure the time interval in days for not performing the host check on the endpoint. When the user connects for the first time the Host Checker runs and the results are saved in IPS. However, for the subsequent logins from the same endpoint, the host checking is not performed and the saved host check result is reused till the expiration of the admin defined time interval.

The first connection from the endpoint never reuses the cached results. The subsequent logins from the same endpoint uses the cached host checker results.

This feature saves the Host Check results for clients connecting from Windows and Mac desktop operating systems. This feature helps in providing faster connection or access to the network.

The Host Checker saved/cached results will be cleared in the following scenarios:

- Change in HC policy configuration such as addition, deletion and modifications
- Change in Active ESAP version
- Change in HC configuration such as periodic interval, disabling the caching feature and role configuration under caching feature
- Server reboot

Limitations

- Periodic host checking, rule monitoring, and remediation are supported only for the first connection when the results are not cached
- Change in Compliance status of the device is not detected if cached results are used for the connection

To configure caching on Host Checker:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Under Options, Store host checking evaluation results enable **Store Host Checking evaluation** results and enter the number of days for not performing the Host Check. The default number of days for storing HC results is 7 days. The supported range is between 1- 30 days.

3. The Admin can also choose to cache results based on the roles assigned:

- **Any role is assigned**- If you select this option, the HC results are cached irrespective of the role assigned.
- **Any of the selected roles is assigned**- If you select this option, the HC results are cached only when the selected role is assigned.



It is recommended to not enable caching for remediation roles because the subsequent logins will be in the remediation role as cached results are used.

The screenshot shows the 'Host Checker' configuration page. Under the 'Options' section, there are several settings:

- 'Perform check every:' is set to 10 minutes.
- '*Client-side process, login inactivity timeout:' is set to 20 minutes (min=1).
- 'Auto-upgrade Host Checker' is checked.
- 'Store host checking evaluation results' is expanded, showing:
 - 'Store Host Checking evaluation results for 7 days' is checked.
 - A note states: 'Enabling this option will allow the server to cache the host checking results. The cached results will be used for host checking evaluation for specified number of days, and rule monitoring and periodic host checking feature will not be applicable.'
 - 'Cache results if any of the roles is assigned' is selected (radio button).
 - 'Cache results only if any of the selected roles are assigned' is unselected (radio button).

At the bottom, there are two lists: 'Available Roles' and 'Selected Roles'. The 'Available Roles' list includes: Users, Guest Admin, Guest, Guest Sponsor, and Guest Wired Restricted. There are 'Add ->' and 'Remove' buttons between the two lists.

4. Click **Save Changes**.

Admission Control Using Network Security Devices

Ivanti Policy Secure also extends Admission control integrations based on alerts. IPS integrates with Next Generation firewalls for threat analysis and once that threats alerts are identified, Ivanti Policy Secure leverages syslog mechanism/REST API mechanism and takes appropriate actions on the user sessions to either terminate or change the role.

- [Juniper SDSN](#)
- [Nozomi Networks](#)
- [IBM QRadar](#)
- [Splunk Enterprise](#)
- [Check Point Next Generation Firewall](#)
- [McAfee ePO Server](#)
- [Fortinet Products](#)

ICS Admission Control Using IPS

Admission control feature is extended to ICS sessions using IF-MAP server. When Firewall/SIEM detects compromised remote devices the Firewall/SIEM sends threat alert to IPS. IPS then instructs ICS to act (For example, terminate session, change roles, disable user account) based on the configured admission control policies.

This section explains how IPS can receive alerts from remote users and provide an action to ICS (remote) based on the configured admission control policies. This feature is supported for the admission control clients, which alerts IPS with VPN Tunneling IP address of endpoints. VPN Tunneling IP Address of the user is mandatory in the received alert/message to identify the user session.

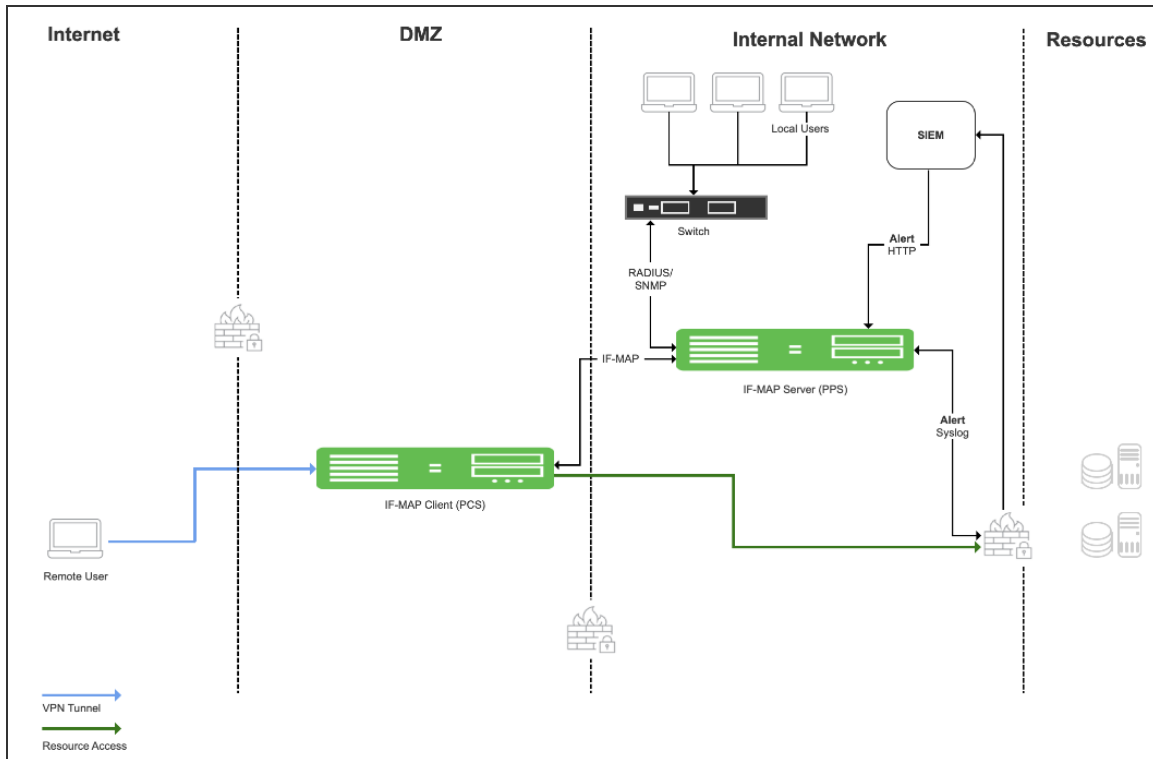


This feature is supported for the admission control clients, which alerts IPS with VPN Tunneling IP address of endpoints. VPN Tunneling IP Address of the user is mandatory in the received alert/message to identify the user session.

The below set of actions can be performed on ICS sessions based on the configured policies:

- Ignore (only log): Received event details are logged and no specific actions are taken.
- Terminate the session: Terminate the user session on the ICS for the received messages.
- Disable the user account: Disable the user on the ICS for the received messages.
- Change user roles: Change the roles assigned to the user on ICS so that restriction/privileges for the user can be changed.

The end user flow is described below:



- Remote user logs in and the user session is created on ICS.
- User session is exported to IF-MAP server (IPS) as fed-wide session.
- User accesses resources and performs a restricted action. For example, accesses a restricted site. The firewall device detects this as a threat and a corresponding event is generated and sent to the IPS.
- IPS looks for the local session if it is available and applies the action based on the policy configured.
- If local session is not available and if Enable Admission Control on Federation-Wide Sessions is enabled, then the policy applies on the fed-wide session.
- ICS IF-MAP client takes the action on local session based on the policy configured.

Configuring ICS Admission Control

1. Administrator configures the required admission control client (like firewalls, SIEMs, EPP etc.) on IPS Admin UI to receive alert/threat information.

2. Select **Endpoint Policy > Admission Control > Configure > Clients > New Client.**
3. **Enable Admission Control on Federation-Wide Sessions.**

Admission Control > Configure > Clients > New Client

New Client

* Name: Label to reference this client.

Description:

* IP Address: IP Address of this client.

* Template: Template used by the client

Selected Template Details

Enable Admission Control for Federation-Wide sessions. Enable Admission Control for other IF-MAP clients(Pulse Connect Secure/Pulse Policy Secure)

Enable IF-MAP Server on this appliance to use Admission Control for Federation-Wide sessions. For Pulse Connect Secure this feature is supported for the Admission Control clients which alerts this appliance with VPN Tunneling IP address of endpoints.

* indicates required field

4. Administrator configures a set of policies that define what actions are to be taken on user sessions, based on the data in the threat events.
5. On IPS Admin UI and ICS Admin UI, administrator enables IF-MAP server under System > IF-MAP > Overview.
6. On ICS Admin UI, administrator enables IF-MAP client under System > IF-MAP > Overview and add IF-MAP server url. Once configured, ICS (IF-MAP client) connects to IF-MAP server (IPS).

i 9.1R12 or later build is required for both Federation client and Fed server to use this feature.

Admission Control is supported with the following vendors:

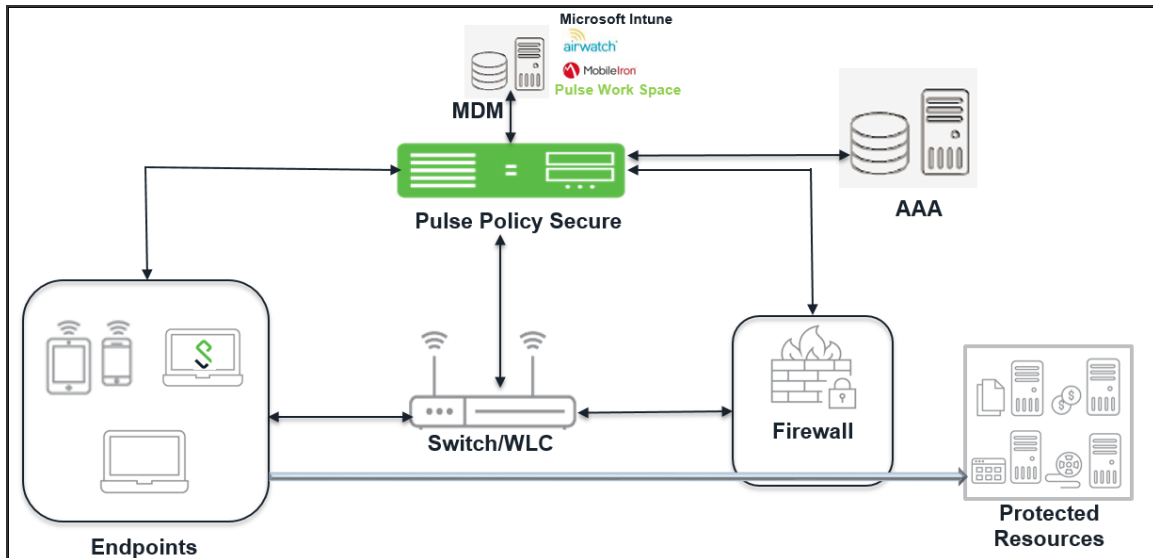
- [Palo Alto Networks Firewall](#)
- [Check Point Next Generation Firewall](#)
- [McAfee ePO Server](#)

MDM Interoperability with IPS

Overview

Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices deployed across mobile operators, service providers, and enterprises. MDM servers consist of a device authorization server that controls the use of some applications on a mobile device (for example, an e-mail application) in the deployed environment. The IPS queries the MDM servers for the necessary device attributes and evaluates them while assigning roles before giving access to the network.

For example, the MDM might detect that a device is out of compliance with IPS role mapping rules. At the next device check interval, IPS queries the MDM for updated attribute data. The compliance check is done periodically and if a formerly compliant device is now non-compliant, it assigns the device the non-compliant role and enforces the same on switch or firewall based on the IPS configuration.



Supported MDM Servers

Ivanti Policy Secure(IPS) supports the following MDM servers:

- Pulse Workspace (PWS)
- Airwatch

- Mobile Iron
- Microsoft Intune

Ivanti Policy Secure(IPS) determines the device identifiers using the following methods:

- Device Certificate
- MAC Address



The dynamic policy evaluation feature is not used in the device access management framework.

The device-attribute-based roles are specified for the following policies:

- 802.1x network access control RADIUS return attribute policies (Layer 2)
- Infranet Enforcer resource policies (Layer 3)

MDM Integration Work Flow

The MDM integration work flow is described below:

1. The user associates a device to SSID.
2. (Optional) If the device is not registered, the user goes through the device on-boarding process.
3. Ivanti Policy Secure(IPS) queries the MDM server with device details through MAC address or device attributes.
4. The MDM server returns device attributes with which IPS uses one or more attributes to determine device access.
5. Ivanti Policy Secure(IPS) allows or denies access based on the attributes.

MDM Dictionary Attributes

This section focuses on the following elements of the MDM configuration that are important to this solution:

- Device identifier—The primary key for device records. Your MDM configuration determines whether a universal unique identifier (UUID), unique device identifier (UDID), or serial number is used as the device identifier.
For AirWatch, UDID is supported and recommended. For MobileIron, UUID is supported and recommended.
- Device attributes—A standard set of data maintained for each device. The device attributes for AirWatch, MobileIron, PWS, and Microsoft Intune are described below.

When the user installs the MDM application on the device and completes enrollment, the MDM pushes the device certificate to the device. After enrollment, the MDM maintains a database record that includes information about the enrollee—attributes related to device identity, user identity, and posture assessment against MDM policies.

Table describes these attributes. In this solution, these attributes are used in IPS role mapping that is the basis for network access and resource access policies. When you configure role-mapping rules, you specify the normalized attribute name.

AirWatch Attribute	Normalized Name	Description	Data Type
BlockLevelEncryption	BlockLevelEncryption	True if block-level encryption is enabled; false otherwise.	Boolean
ComplianceStatus	complianceReason	Values: Compliant, Non-Compliant.	String
ComplianceStatus	isCompliant	True if the status is compliant with MDM policies; false otherwise.	Boolean
CompromisedStatus	CompromisedStatus	True if the status is compromised; false otherwise.	Boolean
CompromisedStatus	isCompromised	True if the device is compromised; false otherwise.	Boolean

AirWatch Attribute	Normalized Name	Description	Data Type
DataProtectionEnabled	DataProtectionEnabled	True if data protection is enabled; false otherwise.	Boolean
DeviceFriendlyName	deviceName	The concatenated name used to identify the device/user combination.	String
EnrollmentStatus	isEnrolled	True if MDM value is Enrolled; false otherwise.	Boolean
FileLevelEncryption	FileLevelEncryption	True if file-level encryption is enabled; false otherwise.	Boolean
Id.Value	deviceId	Device identifier.	String
Imei	IMEI	IMEI number of the device.	String
IsPasscodeCompliant	IsPasscodeCompliant	True if the passcode is compliant with the MDM policy; false otherwise	Boolean
IsPasscodePresent	IsPasscodePresent	True if a passcode has been configured; false otherwise.	Boolean

AirWatch Attribute	Normalized Name	Description	Data Type
LastComplianceCheckOn	LastComplianceCheckOn	The refresh date and timestamp of the last status reported.	Timestamp
LastCompromisedCheckOn	LastCompromisedCheckOn	The refresh date and timestamp of the last status reported.	Timestamp
LastSeen	lastSeen	Date and time the device last made successful contact with the MDM.	Timestamp
LocationGroupName	LocationGroupName	MDM location group configuration value.	String
MacAddress	macAdress	The Wi-Fi MAC address.	String
Model	model	Model is automatically reported by the device during registration.	String
OperatingSystem	osVersion	OS version.	String
Ownership	ownership	Values: C, E, or S (Corporate, Employee, or Shared).	String
PhoneNumber	phoneNumber	Phone number entered during registration.	String

AirWatch Attribute	Normalized Name	Description	Data Type
Platform	platform	Platform specified during registration.	String
SerialNumber	serialNumber	Serial number.	String
Udid	UDID	Unique device identifier.	String
UserEmailAddress	userEmail	E-mail address of device user.	String
UserName	userName	Name of device user.	String
Uuid	UUID	Universal unique identifier.	String

MobileIron Attribute	Normalized Name	Description	Data Type
@id	deviceId	Device identifier.	String
blockedReason	blockedReason	Reason MDM has blocked the device. Can be a multivalued string. Values are: <ul style="list-style-type: none"> AllowedAppControlPolicyOutOfCompliance AppControlPolicyOutOfCompliance DataProtectionNotEnabled DeviceAdminDeactivated DeviceComplianceStatusUnknown DeviceCompliant DeviceCompromised 	String

MobileIron Attribute	Normalized Name	Description	Data Type
		<ul style="list-style-type: none"> • DeviceExceedsPerMailboxLimit • DeviceManuallyBlocked • DeviceNotRegistered • DisallowedAppControlPolicyOutOfCompliance • ExchangeReported • HardwareVersionNotAllowed • OsVersionLessThanSupportedOsVersion • PolicyOutOfDate • RequiredAppControlPolicyOutOfCompliance 	
compliance	complianceReason	<p>MDM policy compliance status. Can be a multivalued string. Values are:</p> <ul style="list-style-type: none"> • AllowedAppControlPolicyOutOfCompliance • AppControlPolicyOutOfCompliance • DataProtectionNotEnabled • DeviceAdminDeactivated • DeviceComplianceStatusUnknown • DeviceCompliant • DeviceCompromised • DeviceExceedsPerMailboxLimit • DeviceManuallyBlocked 	String

MobileIron Attribute	Normalized Name	Description	Data Type
		<ul style="list-style-type: none"> • DeviceNotRegistered • DisallowedAppControlPolicyOutOfCompliance • ExchangeReported • HardwareVersionNotAllowed • OsVersionLessThanSupportedOsVersion • PolicyOutOfDate • RequiredAppControlPolicyOutOfCompliance 	
compliance	isCompliant	True if the device is in compliance with its MDM security policies; false otherwise.	Boolean
compliance	isCompromised	True if the device is compromised; false otherwise.	Boolean
countryName	countryName	Country name corresponding with the country code of the device.	String
currentPhoneNumber	phoneNumber	Phone number entered during registration.	String
emailAddress	userEmail	E-mail address of device user.	String
employeeOwned	Ownership	Values: Employee or Corporate.	String
homeOperator	homeOperator	The service operator for the device when it is not roaming.	String
iPhone IMEI (iOS), imei (Android)	Imei	IMEI number of the device.	String
iPhone UDID	UDID	Unique device identifier.	String

MobileIron Attribute	Normalized Name	Description	Data Type
isBlocked	isBlocked	True if the device is blocked from accessing the ActiveSync server; false otherwise.	Boolean
isQuarantined	isQuarantined	True if the device is quarantined by the MDN; false otherwise.	Boolean
lastConnectAt	lastSeen	Date and time the device last made successful contact with the MDM.	Timestamp
manufacturer	manufacturer	Manufacturer is automatically reported by the device during registration.	String
mdmManaged	mdmManaged	True if the MDM profile is enabled on the device; false otherwise. This field applies only to iOS devices. For other devices, the value is always false.	Boolean
modelName, model, device_ model	Model	Model is automatically reported by the device during registration.	String
name	deviceName	The concatenated name used to identify the device/user combination.	String
operator	Operator	Service provider. The value PDA indicates no operator is associated with the device.	String
OSVersion (iOS), os_version (Android)	osVersion	OS version.	String
platform	Platform	Platform specified during registration.	String
principal	userId	User ID.	String
quarantinedReason	quarantinedReason	MDM policy compliance status. Can be a multivalued string. Values are: <ul style="list-style-type: none"> AllowedAppControlPolicyOutOfCompliance AppControlPolicyOutOfCompliance 	

MobileIron Attribute	Normalized Name	Description	Data Type
		<ul style="list-style-type: none"> • DataProtectionNotEnabled • DeviceAdminDeactivated • DeviceComplianceStatusUnknown • DeviceCompliant • DeviceCompromised • DeviceExceedsPerMailboxLimit • DeviceManuallyBlocked • DeviceNotRegistered • DisallowedAppControlPolicyOutOfCompliance • ExchangeReported • HardwareVersionNotAllowed • OsVersionLessThanSupportedOsVersion • PolicyOutOfDate • RequiredAppControlPolicyOutOfCompliance 	
SerialNumber	serialNumber	Serial number.	String
statusCode	isEnrolled	True if the device has completed enrollment or registration; false otherwise.	Boolean
uuid	UUID	Universal unique device identifier.	String
userDisplayName	userName	Name of device user.	String
wifi_mac (iOS), wifi_mac_addr (Android)	macAdress	The Wi-Fi MAC address.	String

Intune Attribute	Normalized Name	Description	Data Type
complianceState	isCompliant	True or false (string) based on whether device is compliant or non-compliant.	Boolean
isManaged	isEnrolled	True or false (indicating whether the client is managed by Intune or not).	Boolean
macAddress	macAddress	MAC address of the device.	String
serialNumber	serialNumber	Serial number of the device. Applies to iOS Devices only.	String
imei	IMEI	The device unique identifier. IMEI (15 decimal digits: 14 digits plus a check digit) or IMEISV (16 digits) includes information on the origin, model, and serial number of the device.	String
udid	UDID	The device unique identifier. Unique Device Identifier (UDID), which is a sequence of 40 letters and numbers that is specific to iOS devices.	String
meid	MEID	MEID is 56 bits long (14 hex digits). It consists of three fields, including an 8-bit regional code (RR), a 24-bit manufacturer code, and a 24-bit manufacturer-assigned serial number.	String
osVersion	osVersion	OS Version of the device.	String
model	Model	Model of the device.	String

Intune Attribute	Normalized Name	Description	Data Type
manufacturer	manufacturer	Device Manufacturer.	String
azureDeviceId	deviceId	The device Id of the device after it has work place joined with Azure Active Directory.	String
lastContactTimeUtc	lastSeen	The date time when the device last checked in with the Intune management service endpoint.	String The format is MM/DD/YYYY HH:MM:SS

Refer to third-party documentation for complete information and configuration details.

Configuring IPS with MDM Servers

Configuring an Authentication Protocol Set

The authentication protocol set associated with the sign-in page must include the EAP method selected in the MDM Wi-Fi profile. The predefined authentication protocol set named 802.1x can be used as-is because it includes all the EAP methods currently configurable on MDMs.

To configure the authentication protocol set:

1. Select **Signing In > Authentication Protocols to display the configuration page.**
2. Click **New Authentication Protocol** or select the predefined 802.1x set. If anything other than MAC address is used as a device identifier then you must use cert auth and the protocol set has to be used for cert auth.
3. Click **Save.**

Configuring the MDM Authentication Server

The MDM authentication server configuration is used by IPS to communicate with the MDM. In the device access management framework, the MDM server is used as the device authorization server.

To configure the authentication server:


1. Select **Authentication > Auth Servers** to navigate to the authentication server configuration pages.
2. Select **MDM Server** and click **New Server** to display the configuration page.
3. Complete the configuration as described in Table below.
4. Save the configuration.

The screenshot shows the configuration page for an AirWatchMDM server. The breadcrumb trail is 'Auth Servers > AirWatchMDM'. The page title is 'AirWatchMDM'. There is a 'Settings' button. The configuration fields are as follows:

- Name:** AirWatchMDM (Label to reference this server.)
- Type:** Air Watch
- Server Section:**
 - Server Url:** https://apidev-as.Awmdm.com
 - Viewer Url:** https://apidev.awmdm.com/AirWatch/Devices/DeviceDetails/<deviceAttr.deviceId> (Link if...)
 - Request Timeout:** 15 (second...)
- Administrator Section:**
 - Username:** admin
 - Password:** [masked]
 - Tenant Code:** 140vcnmcn
 - Test Connection** button
- Device Identifier Section:**
 - ID Template:** <certDN.CN> (Template for constructing device identifier from certifi...)
 - ID Type:** UDID (Unique Device Identifier), Serial Number, UUID (Universal Unique Identifier)

Examples of ID Templates:
<certDN.CN> First CN from the subject DN
<certAttr.serialNumber> Certificate serial number
<certAttr.altName.xxx> Where xxx can be:
Email The Email alternate name
UPN The Principal Name alternate name
... etc
<certDNText> The complete subject DN
cert-<certDN.CN> The text "cert-" followed by the first CN from the subject DN

Buttons at the bottom: Save Changes, Reset

Settings	Guidelines
Name	Specify a name for the configuration.
Type	Select the MDM server.
Server	
Server Url	<p>Specify the URL for your AirWatch server. This is the URL AirWatch has instructed you to use to access its RESTful Web API (also called a RESTful Web service). The URL for the AirWatch MDM server used in this example has the following form:</p> <p>https://apidev-as.Awmdm.com https://m.mobileiron.net/pulsesecuretest</p> <hr/> <p> You must configure your firewalls to allow communication between these two nodes over port 443.</p> <hr/>
Viewer Url	<p>Specify the URL for the AirWatch report viewer. This URL is used for links from the Active Users page to the AirWatch report viewer. The URL for the AirWatch MDM viewer for this example has the following form:</p> <p><a href="https://apidev.awmdm.com/AirWatch/Devices/DeviceDetails/<deviceAttr.deviceId>">https://apidev.awmdm.com/AirWatch/Devices/DeviceDetails/<deviceAttr.deviceId> https://m.mobileiron.net/pulsesecuretest/admin/admin.html#smartphones:all</p>
Request Timeout	<p>Specify a timeout period (0-60 seconds) for queries to the MDM server. The default is 15 seconds.</p> <p>Calibrate this value based on your observations on how long a query to the MDM server takes over your network. If your network experiences latency when querying the MDM cloud service, increase the timeout to account for the latency. The system queries the MDM when a user attempts to sign in. If a timeout occurs, role mapping proceeds without attributes.</p>
Administrator	
Username	Specify the username for an account that has privileges to access the MDM RESTful Web API.
Password	Specify the corresponding password.
Tenant Code	Copy and paste the AirWatch API tenant code.
Device Identifier	

Settings	Guidelines
Device identity	<p>Select an option on whether to require that the MDM certificate is presented by the endpoint when signing in:</p> <ul style="list-style-type: none"> • Require — Require that the device certificate pushed to client devices during enrollment be used at sign-in. If this option is selected, and the client device does not have a certificate, authorization fails. Use this option when you require endpoints to adhere to your certificate security requirements. • Use Certificate if present — Use the certificate to derive the device ID if the certificate is presented at sign-in, but do not reject authentication if the certificate is not present. You can use this option in conjunction with a role mapping rule and a remediation VLAN to identify devices that have not perfected MDM enrollment. • Always Use MAC address — In some cases, the MDM certificate might be configured without a device identifier. When the endpoint uses an 802.1x framework to authenticate, IPS can obtain the MAC address from the RADIUS return attribute callingStationID. The system can then use the MAC address as the device identifier.
ID Template	<p>Construct a template to derive the device identifier from the certificate attributes. The template can contain textual characters as well as variables for substitution. The variables are the same as those used in role mapping custom expressions and policy conditions. Enclose variables in angle brackets like this <variable>.</p> <p>For example, suppose the certificate DN is: CN= <EnrollmentUser>, serialNumber= <DeviceUid>, o=Company. With this configuration, the certificate could identify both the user and the device. In this example, the device ID template is <certDN.serialNumber>.</p>
ID Type	<p>Select the device identifier type that matches the selection in the MDM certificate configuration:</p> <ul style="list-style-type: none"> • UUID— The device universal unique identifier. This is the key device identifier supported by MobileIron MDM. • Serial Number—The device serial number. • UDID—The device unique device identifier. This is supported by the AirWatch MDM.

Configuring the Certificate Server

The certificate server configuration enables device users to authenticate using the certificate pushed to the device by the MDM. The certificates are used for user authentication, and the users do not have to enter user credentials.

To configure authentication with the certificate server:

- 1. Select **Authentication > Auth. Servers**.
- 2. Select **Certificate Server** and click **New Server** to display the configuration page.
- 3. Complete the configuration as described in table below.
- 4. Save the configuration.

Auth Servers > New Certificate Server

New Certificate Server

*Name: Label to r

User Name Template: Template

The template can contain textual characters as well as variables for custom expressions and policy conditions. All of the certificate variables are defined in the following table.

Examples:	
<certDN.CN>	First CN from the subject DN
<certAttr.serialNumber>	Certificate serial number
<certAttr.altName.xxx>	Where xxx can be:
	Email The Email alternate name
	UPN The Principal Name alternate name
	... etc
<certDNText>	The complete subject DN
cert-<certDN.CN>	The text "cert-" followed by the first CN from the sub

▼ User Record Synchronization

Enable User Record Synchronization

Logical Auth Server Name:

* indicates required field

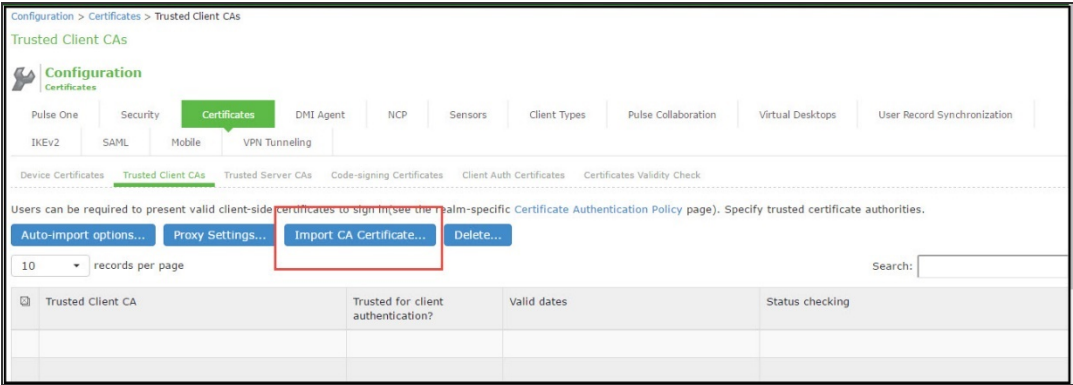
Settings	Guidelines
Name	Specify a name to identify the server within the system.
User Name Template	<p>Specify a username template. Specify how the system should construct a username. You may use any combination of certificate variables contained in angle brackets and plain text. The username template you configure must be consistent with the MDM certificate template configuration. Your goal is to identify the values specified in the MDM certificate that are to be used as the username in IPS system. This value populates the <USER> and <USERNAME> session variables for use throughout the rest of the system configuration.</p> <p>For example, suppose the certificate DN is: CN=<EnrollmentUser>, serialNumber=<DeviceUid>, o=Company. With this configuration, the certificate could identify both the user and the device. In this example, the username template is <certDN.CN>.</p>

Adding the MDM Certificate to the Trusted Client CA Configuration

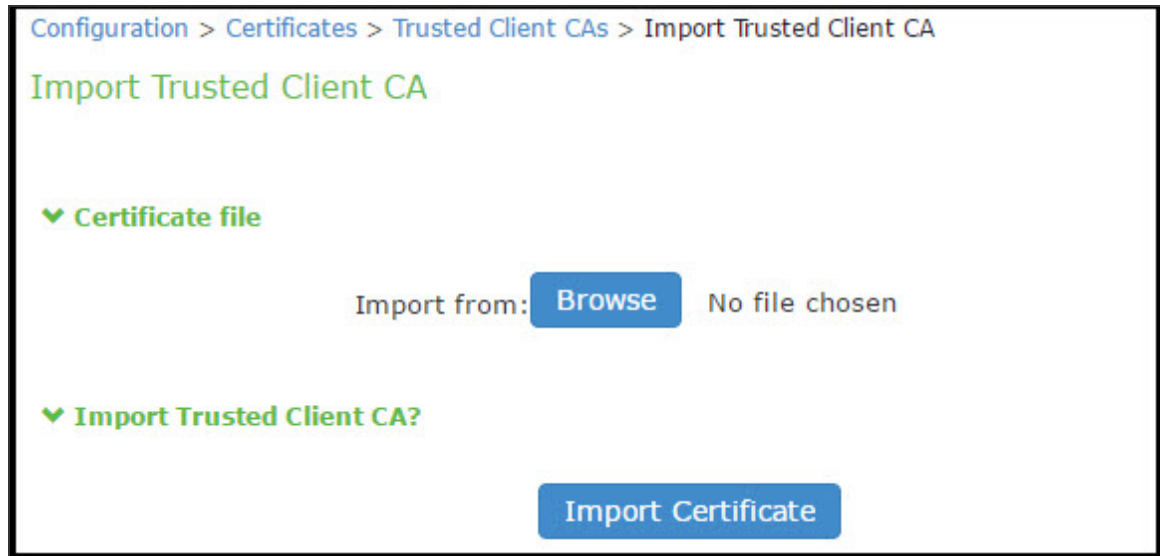
The system uses the uploaded certificate to verify that the browser-submitted certificate is valid. You must upload the MDM certificate that signed the client certificate that was pushed to the mobile devices. Typically, you obtain this certificate from the MDM when your company establishes its account with them.

To import a trusted client CA certificate:

1. Select **System > Configuration > Certificates > Trusted Client CAs**.



2. Click **Import Trusted Client CA Certificate**.



3. Browse to the certificate file, select it, and click Import Certificate to complete the import operation.
4. Click the link for the Trusted Client CA to display its details.

Configuring User Roles

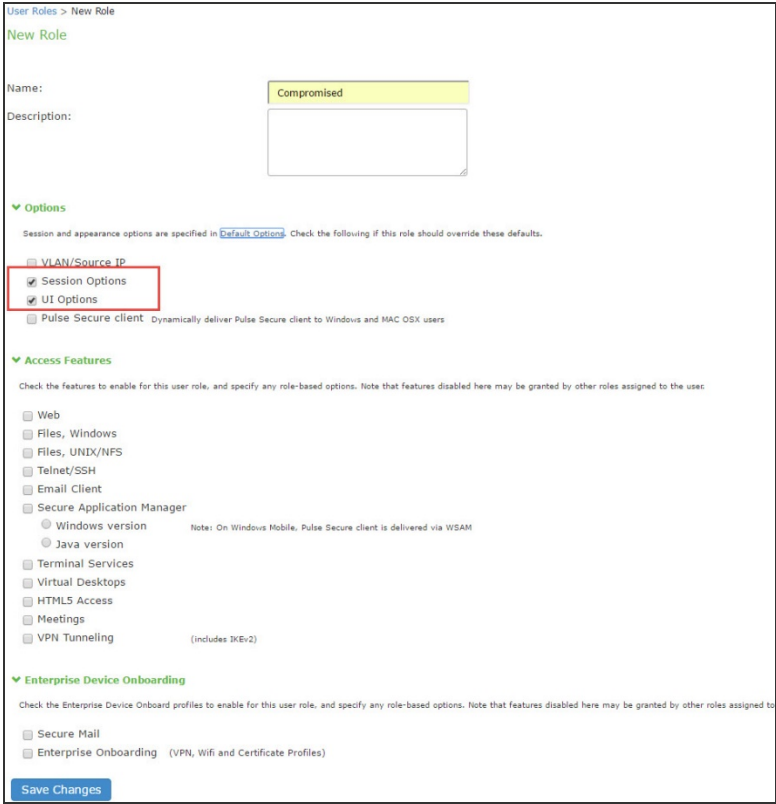
User roles are classifiers for network access control policies. You create a set of roles to use in your classification scheme: device status is MDM enrollment complete or incomplete; device status is MDM-policy compliant or noncompliant; device is employee owned or company owned; device platform is iOS, Android, or neither; and so forth.

The user role configuration also includes options to customize user interface features that are appropriate for a particular role. For MDM deployments, you can use the Personalized Greeting UI option to send a notification message to the device when the role has been applied.

To configure user roles:

1. Select **Users > User Role** to navigate to the role configuration page.
2. Click **New Role** to display the configuration page.
3. Complete the configuration for general options as described in below table.
4. Save the configuration.

- 5. Click **UI options** to display the configuration page.
- 6. Complete the configuration for UI options as described in below table.
- 7. Save the configuration.
- 8. Click **Session Options** to display the configuration page.
- 9. Complete the configuration for session options as described in below table.
- 10. Save the configuration.
- 11. Click **Agentless** to display the configuration page.
- 12. Complete the configuration for agentless options as described in below table.
- 13. Save the configuration.



User Roles > Compromised > General > UI Options

UI Options

General Web Files SAN Telnet/SSH Terminal Services Virtual Desktops HTML5 Access Meetings VPN Tunneling

Enterprise Onboarding

Overview Restrictions VLAN/Source IP Session Options **UI Options**

Save Changes Restore Factory Defaults

Header

Current appearance: Pulse Secure

Logo image: No file chosen Recommended size: Less than 40 pixels tall and 100B.

Background color: #E3E3E3

Sub headers

Current appearance: Label

Background color: #336699

Text color: #FFFFFF

Start page

The start page determines where a user starts after signing in.

Bookmarks page

Welcome message:

Portal Name:

Meetings page

Custom page

Start page URL: Example: http://www.domain.com/

Also allow access to directories below this url

Bookmarks Panel Arrangement

Determine the location and order of panels on the user's bookmarks page. Note that all panels may not be displayed.

Left Column	Right Column
<input type="button" value="Move Up"/> Welcome	<input type="button" value="Move >"/> HTML5 Access Ses
<input type="button" value="Move Down"/> Web Bookmarks	<input type="button" value="< Move"/>
Files	
Terminal Sessions	
Client Application S	
Virtual Desktops	

Help Page

Disable help link

Standard help page

Custom help page

Help page URL: Example: http://www.domain.com/help

Also allow access to directories below this url

Window size: width height

User Toolbar

Determine the tools that are available to users at the top of the secure gateway pages on the IVE.

Home

Preferences

Session Counter

Client Application Sessions

If this is not displayed on the toolbar, it will be displayed as a panel on the user's home page.

Browsing toolbar

Determine the tools that are available to users when browsing pages not located on the IVE, such as external web sites.

Show the browsing toolbar

Toolbar type: Standard Framed

Toolbar logo: No file chosen Recommended size: Less than 24 pixels tall and 6KB

Toolbar logo (mobile): No file chosen Recommended size: Less than 12 pixels tall and 3KB

Logo links to:

Bookmarks page

"Start Page" settings

Custom URL: An access control rule will be created for this url.

Also allow access to directories below this url

Enable "Home" link

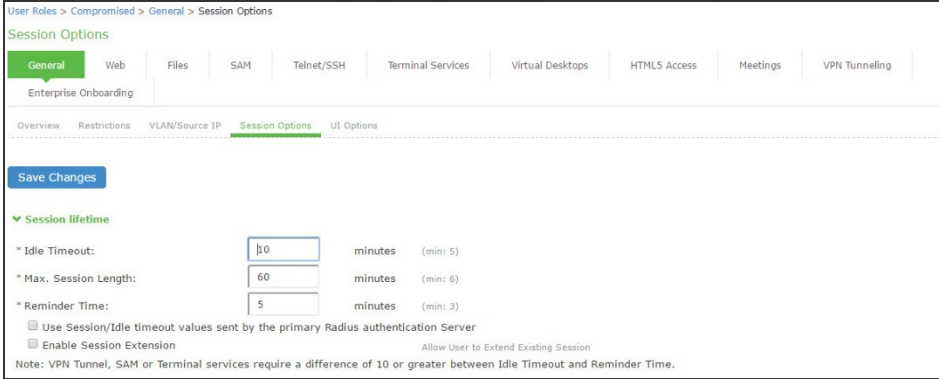
Enable "Add Bookmark" link

Enable "Bookmark Favorites" link

Display Session Counter

Enable "Help" link

Use iFrame in Toolbar



Settings	Guidelines
Overview tab	
Name	Specify a name for the configuration.
Description	Describe the purpose of the role so that other administrators are aware of it.
Options	Select UI Options so that you can customize a message to be sent to the device when the role is applied.
UI Options tab	
Personalized greeting	<p>Select the Show notification message option and enter a message to be sent to the device (through the MDM API) after sign-in and this role has been applied, or after role reevaluation if it results in a role change to this role.</p> <p>In this example, we are using the system to enforce MDM enrollment by flagging compromised devices. The message, therefore, is: Your device is compromised. Network access may be limited.</p> <p>The message is forwarded to the device using the MDM server Push Notification feature.</p> <p>The content of your notification message can vary depending on whether the switch or access point supports change of authorization (CoA). If the CoA is supported, reauthentication is automatic, so your message might simply state that "your level of access has changed." If CoA is not supported, reauthentication needs to be done manually by the user in which case the message might state that "your level of access has changed, please reconnect."</p> <p>NOTE: When multiple roles are assigned, UI options are not merged. The UI options for the first role that matches are applied.</p>
Session Options	

Settings	Guidelines
Allow VPN Through Firewall	Enable this option to allow Infranet Enforcer traffic to act as a heartbeat and keep the session alive. This option is useful for iOS devices.
Agentless	
Enable agentless access	Select this option for roles that you provision to access the network from BYOD devices. The solution that integrates with MDMs depends on the native supplicant, not an Ivanti agent.

Configuring a Realm and Role Mapping Rules

The user realm configuration associates the authentication server data and MDM server data with user roles.

To configure the realm and role mapping rules:

1. Select **Users > User Realms > New User Realm** to display the configuration page.
2. Upon saving the new realm, the system displays the role mapping rules page.
3. Click **New Rule** to display the configuration page.
4. Complete the configuration as described in table.
5. Click the **Authentication Policy** tab and then click the **Certificate subtab** to display the certificate restriction configuration page.

Settings	Guidelines
Name	Specify a name for the realm. If you enable sign-in using a realm suffix in the sign-in policy configuration, the realm name must match the username realm suffix configured in the MDN Wi-Fi profile.
Description	Describe the purpose of the realm so that other administrators are aware of it.
Servers	

Settings	Guidelines
Authentication	Select the user authentication server for this realm’s users. This example uses the certificate server configured in the earlier step. When you use a certificate server, users are not prompted for their credentials. You can also select the authentication server used for employees. In that case, users are prompted by the sign-in page to provide their username and password.
User Directory/Attribute	This option is not used.
Accounting	This option is not used.
Device Attributes	Select the MDM server configured for device authorization.
Device Check Interval	<p>Select this feature to leverage the MDM posture assessment checks and enforce compliance. For example, the MDM might detect that a device is out of compliance with its security policies, such as a password policy. At the next device check interval, IPS queries the MDM for updated attribute data. In this example, it learns that a formerly compliant device is now noncompliant. It assigns the device the noncompliant role and sends the 802.1x authenticator the corresponding RADIUS attribute to place it in a remediation VLAN.</p> <p>Specify the interval at which to query the MDM for updated attribute data. Specify 0 to disable periodic queries. The minimum is 10 minutes and the maximum is 10080 minutes (7 days).</p> <p>Specify an interval that is appropriate for the MDM. Some MDMs, for example, update records every 4 hours, so a 10-minute interval would not be productive.</p>
Dynamic Policy Evaluation	
Dynamic Policy Evaluation	This option is not used.

User Realms > All Roles Realm - NC Client > Role Mapping > Role Mapping Rule

Role Mapping Rule

* Name:

▼ Rule:if username...

If more than one username should match, enter one username per line. You can use * wildcards.

▼ then assign these roles

Available Roles:

- AAA QA Role
- Client QA Role
- Core QA Role
- Default QA VLAN Role
- JSAM Role

Add ->

Remove

Selected Roles:

- Terminal Services Role
- Web Role
- STA Role
- WSAM Role
- HTML5 Role

Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

Settings	Guidelines
Rule based on	Select Device Attribute and click Update to update the configuration page so that it displays settings for role mapping using device attributes.
Name	Specify a name for the configuration.
Rule	Select a device attribute and a logical operator (is or is not), and type a matching value or value pattern. In this example, select isCompromised and the logical operator is, and enter the value 1 (true). This means that devices with a compromised status match the rule.
Role assignment	Select the roles to apply if the data matches the rule.

The following table describes the AirWatch record attributes that can be used in role mapping rules.

Role Mapping Attribute Name	AirWatch Attribute Name	Description	Data Type
BlockLevelEncryption	BlockLevelEncryption	True if block-level encryption is enabled; false otherwise.	Boolean
complianceReason	ComplianceStatus	Values: Compliant, Non-Compliant.	String
CompromisedStatus	CompromisedStatus	True if the status is compromised; false otherwise.	Boolean
DataProtectionEnabled	DataProtectionEnabled	True if data protection is enabled; false otherwise.	Boolean
deviceId	Id.Value	Device identifier.	String
deviceName	DeviceFriendlyName	The concatenated name used to identify the device/user combination.	String
FileLevelEncryption	FileLevelEncryption	True if file-level encryption is enabled; false otherwise.	Boolean
IMEI	Imei	IMEI number of the device.	String
isCompliant	ComplianceStatus	Values: Compliant.	String

Role Mapping Attribute Name	AirWatch Attribute Name	Description	Data Type
isCompromised	CompromisedStatus	True if the device is compromised; false otherwise.	Boolean
isEnrolled	EnrollmentStatus	True if MDM value is Enrolled; false otherwise.	Boolean
IsPasscodeCompliant	IsPasscodeCompliant	True if the passcode is compliant with the MDM policy; false otherwise	Boolean
IsPasscodePresent	IsPasscodePresent	True if a passcode has been configured; false otherwise.	Boolean
LastComplianceCheckOn	LastComplianceCheckOn	The refresh date and timestamp of the last status reported.	Timestamp
LastCompromisedCheckOn	LastCompromisedCheckOn	The refresh date and timestamp of the last status reported.	Timestamp
lastSeen	LastSeen	Date and time the device last made successful contact with the MDM.	Timestamp

Role Mapping Attribute Name	AirWatch Attribute Name	Description	Data Type
LocationGroupName	LocationGroupName	MDM location group configuration value.	String
macAdress	MacAddress	The Wi-Fi MAC address.	String
model	Model	Model is automatically reported by the device during registration.	String
osVersion	OperatingSystem	OS version.	String
ownership	Ownership	Values: C, E, or S (Corporate, Employee, or Shared).	String
phoneNumber	PhoneNumber	Phone number entered during registration.	String
platform	Platform	Platform specified during registration.	String
serialNumber	SerialNumber	Serial number.	String
UDID	Udid	Unique device identifier.	String
userEmail	UserEmailAddress	E-mail address of device user.	String
userName	UserName	Name of device user.	String

Role Mapping Attribute Name	AirWatch Attribute Name	Description	Data Type
UUID	Uuid	Universal unique identifier.	String

The following table describes the MobileIron record attributes that can be used in role mapping rules.

Role Mapping Attribute Name	MobileIron Attribute Name	Description	Data Type
blockedReason	blockedReason	Reason MDM has blocked the device. Can be a multivalued string. Values are: <ul style="list-style-type: none"> • AllowedAppControlPolicyOutOfCompliance • AppControlPolicyOutOfCompliance • DataProtectionNotEnabled • DeviceAdminDeactivated • DeviceComplianceStatusUnknown • DeviceCompliant • DeviceCompromised • DeviceExceedsPerMailboxLimit • DeviceManuallyBlocked • DeviceNotRegistered • DisallowedAppControlPolicyOutOfCompliance • ExchangeReported • HardwareVersionNotAllowed • OsVersionLessThanSupportedOsVersion 	String

Role Mapping Attribute Name	MobileIron Attribute Name	Description	Data Type
		<ul style="list-style-type: none"> • PolicyOutOfDate • RequiredAppControlPolicyOutOfCompliance 	
complianceReason	compliance	<p>MDM policy compliance status. Can be a multivalued string. Values are:</p> <ul style="list-style-type: none"> • AllowedAppControlPolicyOutOfCompliance • AppControlPolicyOutOfCompliance • DataProtectionNotEnabled • DeviceAdminDeactivated • DeviceComplianceStatusUnknown • DeviceCompliant • DeviceCompromised • DeviceExceedsPerMailboxLimit • DeviceManuallyBlocked • DeviceNotRegistered • DisallowedAppControlPolicyOutOfCompliance • ExchangeReported • HardwareVersionNotAllowed • OsVersionLessThanSupportedOsVersion • PolicyOutOfDate • RequiredAppControlPolicyOutOfCompliance 	String

Role Mapping Attribute Name	MobileIron Attribute Name	Description	Data Type
countryName	countryName	Country name corresponding with the country code of the device.	String
deviceId	@id	Device identifier.	String
deviceName	name	The concatenated name used to identify the device/user combination.	String
homeOperator	homeOperator	The service operator for the device when it is not roaming.	String
imei	iPhone IMEI (iOS), imei (Android)	IMEI number of the device.	String
isBlocked	isBlocked	True if the device is blocked from accessing the ActiveSync server; false otherwise.	Boolean
isCompliant	compliance	True if the device is in compliance with its MDM security policies; false otherwise.	Boolean
isCompromised	compliance	True if the device is compromised; false otherwise.	Boolean
isEnrolled	statusCode	True if the device has completed enrollment or registration; false otherwise.	Boolean
isQuarantined	isQuarantined	True if the device is quarantined by the MDN; false otherwise.	Boolean
lastSeen	lastConnectAt	Date and time the device last made successful contact with the MDM.	Timestamp
manufacturer	manufacturer	Manufacturer is automatically reported by the device during registration.	String
macAddress	wifi_mac (iOS), wifi_mac_addr (Android)	The Wi-Fi MAC address.	String

Role Mapping Attribute Name	MobileIron Attribute Name	Description	Data Type
mdmManaged	mdmManaged	True if the MDM profile is enabled on the device; false otherwise. This field applies only to iOS devices. For other devices, the value is always false.	Boolean
model	ModelName, model, device_model	Model is automatically reported by the device during registration.	String
operator	operator	Service provider. The value PDA indicates no operator is associated with the device.	String
osVersion	OSVersion (iOS), os_version (Android)	OS version.	String
ownership	employeeOwned	Values: Employee or Corporate.	String
phoneNumber	currentPhoneNumber	Phone number entered during registration.	String
platform	platform	Platform specified during registration.	String
quarantinedReason	quarantinedReason	MDM policy compliance status. Can be a multivalued string. Values are: <ul style="list-style-type: none"> AllowedAppControlPolicyOutOfCompliance AppControlPolicyOutOfCompliance DataProtectionNotEnabled DeviceAdminDeactivated DeviceComplianceStatusUnknown DeviceCompliant DeviceCompromised DeviceExceedsPerMailboxLimit 	

Role Mapping Attribute Name	MobileIron Attribute Name	Description	Data Type
		<ul style="list-style-type: none"> • DeviceManuallyBlocked • DeviceNotRegistered • DisallowedAppControlPolicyOutOfCompliance • ExchangeReported • HardwareVersionNotAllowed • OsVersionLessThanSupportedOsVersion • PolicyOutOfDate • RequiredAppControlPolicyOutOfCompliance 	
serialNumber	SerialNumber	Serial number.	String
UDID	iPhone UDID	Unique device identifier.	String
userEmail	emailAddress	E-mail address of device user.	String
userId	principal	User ID.	String
userName	userDisplayName	Name of device user.	String
UUID	uuid	Universal unique device identifier.	String

Role Mapping Attribute Name	PWS Attribute Name	Description	Data Type
osVersion	os_version	OS version	String
UUID	uuid	Unique device identifier	String

Role Mapping Attribute Name	PWS Attribute Name	Description	Data Type
IMEI	imei	IMEI number of the device.	String
macAddress	wifi_mac	The Wi-Fi MAC address.	String
serialNumber	serial_number	Serial number of the device.	String
lastSeen	last_seen	Date and time the device last made successful contact with the MDM.	Time Stamp
isCompliant isCompromised complianceReason	is_compliant	True if the device is in compliance with its MDM security policies; false otherwise.	Boolean
isEnrolled	state	True or false (indicating whether the client is managed by PWS or not).	Boolean
UDID	ios_udid	The device unique identifier. Unique Device Identifier (UDID), which is a sequence of 40 letters and numbers that is specific to iOS devices.	String
model	model	Model of the device.	String

Role Mapping Attribute Name	PWS Attribute Name	Description	Data Type
phonenumber	PhoneNumber	Phone number entered during registration.	String
userName	username	Name of device user.	String
carrier	carrier	User ID.	String
manufacturer	manufacturer	Device manufacturer name.	String
deviceName	devicename	Name of the device.	String

Role Mapping Attribute Name	Microsoft Intune Attribute Name	Description	Data Type
deviceid	azureDeviceId	The device Id of the device after it has work place joined with Azure Active Directory.	String
IMEI	imei	The device unique identifier. IMEI (15 decimal digits: 14 digits plus a check digit) or IMEISV (16 digits) includes information on the origin, model, and serial number of the device.	String
isCompliant	complianceState	True or false (string) based on whether device is compliant or non-compliant.	Boolean

Role Mapping Attribute Name	Microsoft Intune Attribute Name	Description	Data Type
isEnrolled	isManaged	True or false (indicating whether the client is managed by Intune or not).	Boolean
lastSeen	lastContactTimeutc	The date time when the device last checked in with the Intune management service endpoint.	String The format is MM/DD/YYYY HH:MM:SS
macAddress	macAddress	MAC address of the device.	String
manufacturer	manufacturer	Device Manufacturer.	String
meid	meid	MEID is 56 bits long (14 hex digits). It consists of three fields, including an 8-bit regional code (RR), a 24-bit manufacturer code, and a 24-bit manufacturer-assigned serial number.	String
model	model	Model of the device.	String
osVersion	osVersion	OS Version of the device.	String
serialNumber	serialNumber	Serial number of the device. Applies to iOS Devices only.	String
UDID	udid	The device unique identifier.	String

Role Mapping Attribute Name	Microsoft Intune Attribute Name	Description	Data Type
		Unique Device Identifier (UDID), which is a sequence of 40 letters and numbers that is specific to iOS devices.	
UUID	uuid	Universal unique device identifier.	String

User Realms > All Roles Realm - NC Client > Authentication Policy > Certificate

Certificate

General **Authentication Policy** Role Mapping

Source IP Browser **Certificate** Password Host Checker Limits

- Allow all users (no client-side certificate required)
- Allow all users and remember certificate information while user is signed in.
- Only allow users with a client-side certificate signed by Trusted Client CAs to sign in. To change the certification authority, see the [Trusted Client CA](#) page

You can optionally require specific values in the client certificate:

10 records per page

Certificate field (example "cn")	Expected value
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

[Save Changes](#)

Settings	Guidelines
Allow all users	Do not select this option. If you select this option, the system does not request a client certificate during the TLS handshake.

Settings	Guidelines
Allow all users and remember certificate	If you select this option, the system requests a client certificate during the TLS handshake. It does allow endpoints to authenticate without a client certificate. For those with a client certificate, the certificate attributes are placed in the session context.
Only allow users with a client-side certificate	If you select this option, the system requests a client certificate during the TLS handshake. It does not allow endpoints to authenticate without a valid client certificate. If the realm is configured with a certificate server, like this example, this option is the only option that can be selected.

Configuring a Sign-In Policy

A sign-in policy associates devices with a realm.

To configure a sign-in policy:

1. Select **Authentication > Signing In > Sign-In Policies** to navigate to the sign-in policies configuration page.
2. Click **New URL** to display the configuration page.
3. Complete the configuration as described below.
4. Save the configuration.

Settings	Guidelines
User type	Select Users.
Sign-in URL	Enter a URL.
Description	Describe the purpose of the sign-in policy so that other administrators are aware of it.
Sign-In Page	Select a sign-in page.
Authentication Realm	
Realm	Select the realm you configured in the earlier step.

Settings	Guidelines
Authentication Protocol Set	Select the protocol you configured in the earlier step.
Realm name as a username suffix	<p>Select this option if the username sent during sign-in includes a realm suffix. To use this option, the realm name must match the username realm suffix configured in the MDM Wi-Fi profile.</p> <p>This configuration enables you to dedicate the realm to the MDM traffic. Non-MDM traffic passing through the same switch then belongs to a different realm.</p> <p>NOTE: In some cases, you can use authentication protocol sets to segregate traffic into a particular realm. For example, assuming only mobile endpoints use TLS and other endpoints do not, an authentication protocol set containing only TLS can be created and associated with a particular realm through a sign-in policy.</p>
Remove realm suffix	Remove the realm suffix within system processes, such as rule processing and logs.

Configuring IPS with Pulse Workspace

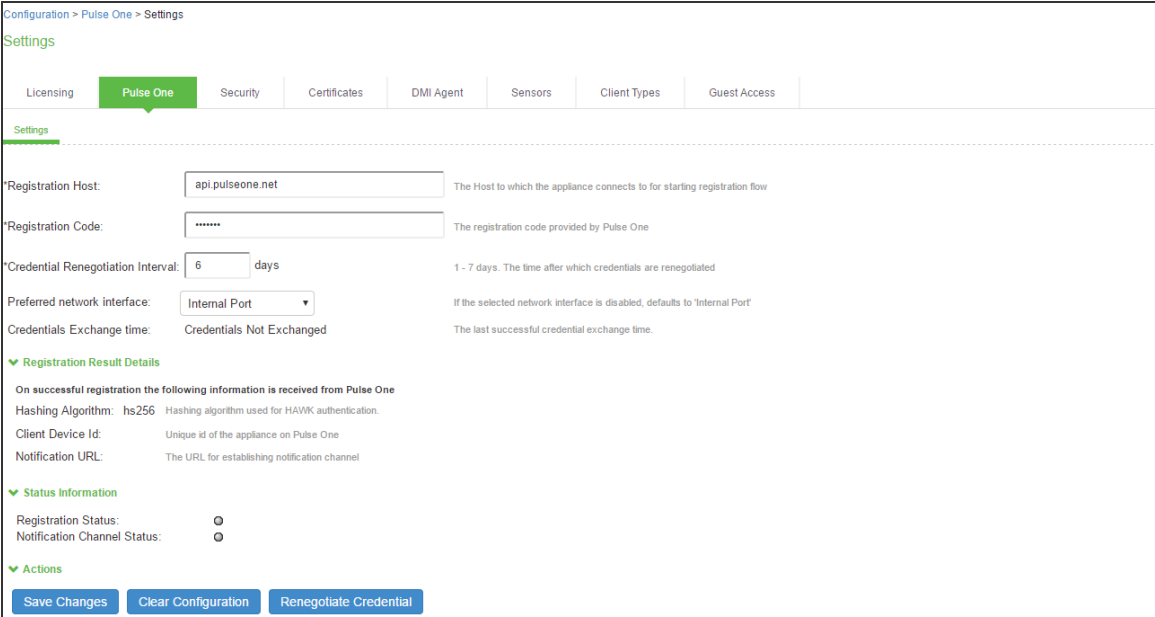
Pulse Workspace is the Ivanti MDM server which provides the device compliance status for the mobile devices. IPS retrieves the device attributes from PWS and uses it for compliance assessments and role assignment.

To configure PWS MDM:

1. Select **System > Configuration > Pulse One > Settings** to register IPS with Pulse One.
2. Enter the **PWS registration URL** and registration code details and register IPS to PWS.

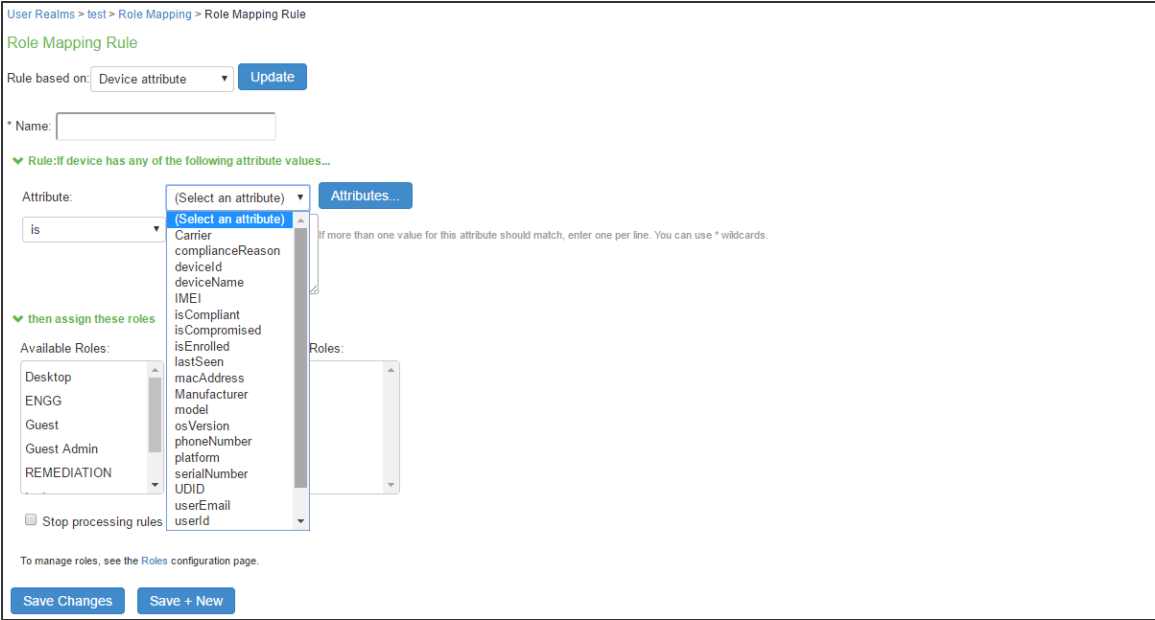
- 3. Click **Save Changes**.

The registration status and the notification channel status turns green if the connection is successful.



- 4. Select **Authentication > Auth. Servers > New MDM Server**. Enter the name, select Pulse Workspace as **MDM** and click **Save changes**.
- 5. Select **Users > User Realms** and select the **Device Attribute server for PWS**.

- 6. Select **Role Mapping** tab of the user realm to create role mapping rules. Configure the role mapping rules based on the PWS supported device attributes.



Configuring IPS with Microsoft Intune

Microsoft Intune is an MDM server which provides the device compliance status for the mobile devices. IPS retrieves the device attributes from Microsoft Intune and uses it for compliance assessments and role assignment. This feature integrates Microsoft Intune and IPS for providing compliance check and onboarding of devices.

To configure Microsoft Intune MDM server:

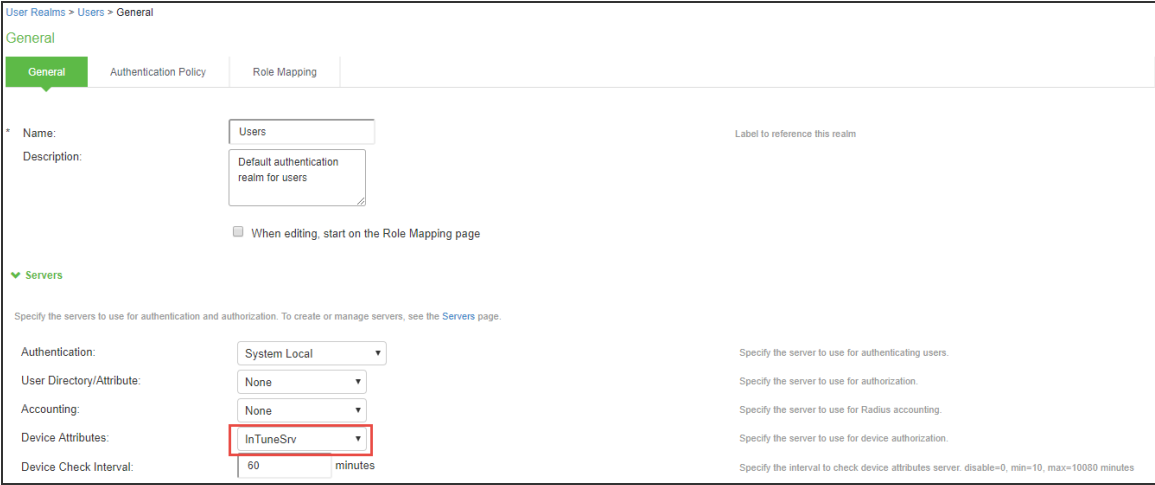
1. Select **Authentication > Auth. Servers > New MDM Server**.
2. Enter the server name, select Microsoft Intune as MDM.
 - Enter the Azure AD Tenant ID.
 - Enter the Web application ID or Client ID that is registered in Azure AD.
 - Enter the Client Secret key registered in the Azure AD.
 - Enter the Timeout duration in seconds. Default is 15 seconds.

To obtain Tenant ID, Client ID, Client Secret Key, see [Viewing Client ID, Tenant ID, and Client Secret](#).

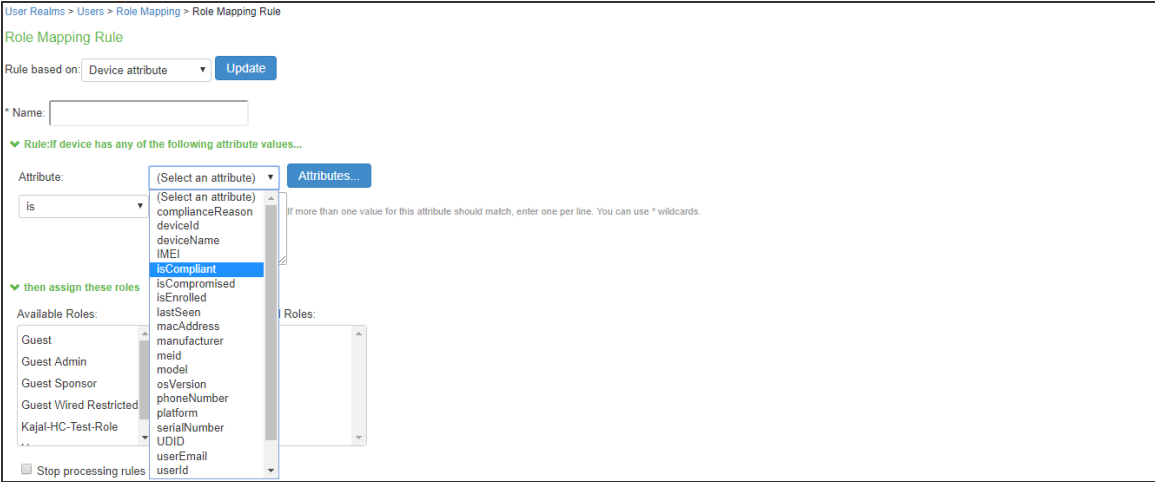
3. Click **Save changes**.

The screenshot shows the 'New MDM Server' configuration page. At the top, it says 'Auth Servers > New MDM Server' and 'New MDM Server'. There is a text input field for '*Name:' with a placeholder 'Label to reference this server.'. Below this is a 'Type:' section with radio buttons for 'Pulse Workspace', 'Air Watch', 'Mobile Iron', and 'Microsoft Intune' (which is selected). A 'Server' section is expanded, showing four required fields: '* Tenant ID:' (with a placeholder 'Azure AD Tenant ID'), '* Client ID:' (with a placeholder 'Web application ID that has been registered in azure AD'), '* Client Secret:' (with a placeholder 'Secret key of the web application registered in azure AD'), and '* Request Timeout:' (with a value of '15' and a placeholder 'seconds (5 - 60)'). There is a 'Test Intune Connection' button. At the bottom, there are 'Save Changes' and 'Reset' buttons. A note at the bottom states: 'Note: Pulse Policy Secure uses endpoint's MAC address to query attributes from Microsoft Intune MDM auth server.' A legend indicates that an asterisk '*' indicates a required field.

4. Select **Users > User Realms** and select the **Device Attribute** server for Microsoft Intune.



5. Select **Role Mapping** tab of the user realm to create role mapping rules. Configure the role mapping rules based on the Microsoft Intune supported device attributes.

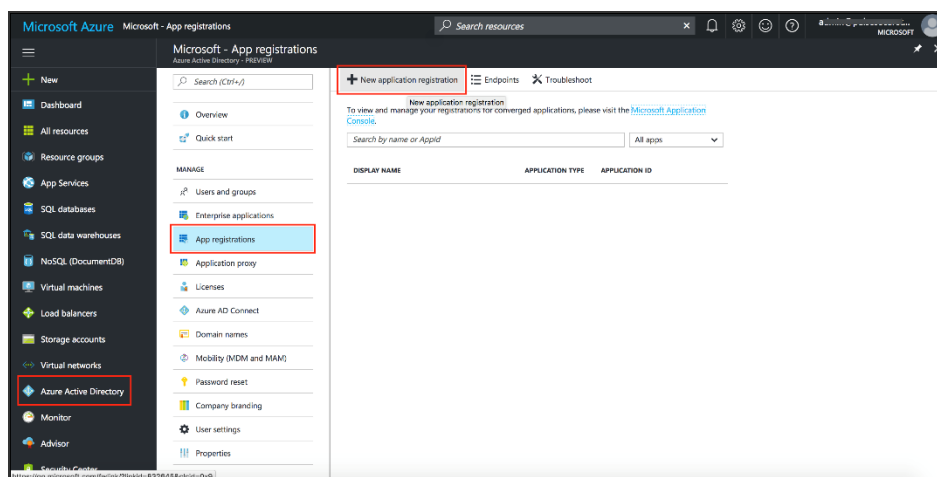


Configuring the Microsoft Intune MDM

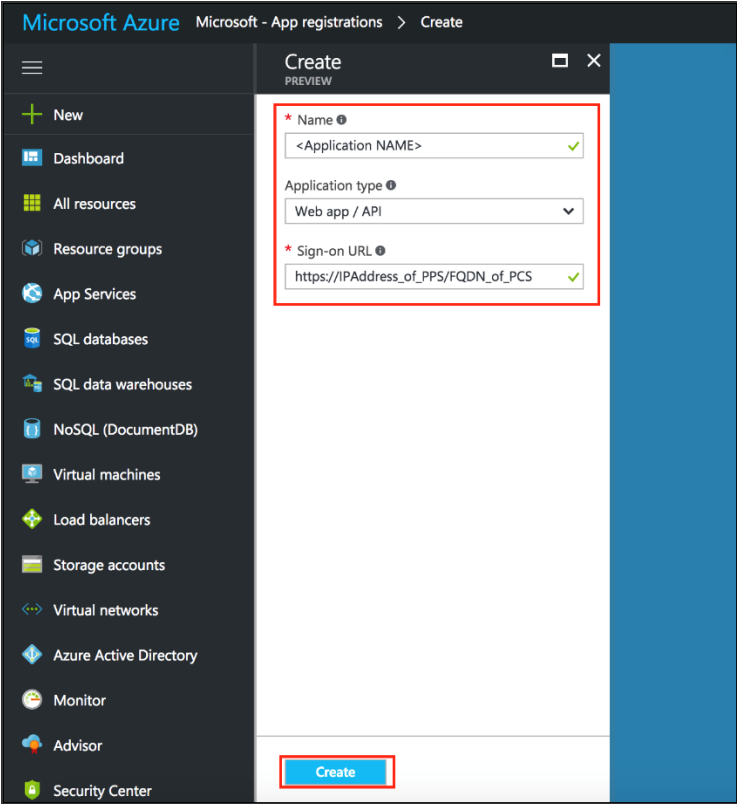
Microsoft Intune acts as the Mobile Device Management (MDM) Server for IPS solution. IPS users have to register their mobile devices with Microsoft Intune. As part of registration, the relevant Profiles get automatically provisioned to mobile device.

To configure the Microsoft Intune MDM:

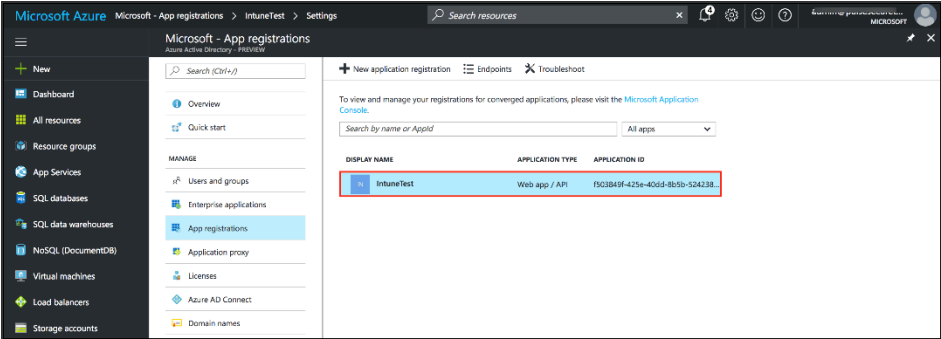
1. Enroll the devices with the MDM server.
2. Create an enterprise WiFi profile.
3. Configure IPS with a role and realm for the user. Microsoft Intune provides the user with a link to provision the created policy and then pushes the profile information. IPS does the role assignment and either allows or denies based on the device assessment. For more information, see [Configuring IPS](#)
4. Create Azure Active Directory (AAD) web application.
5. Go to portal.azure.com, click on the Azure Active Directory on the left of the screen, click on to App registrations and click on New application registration.



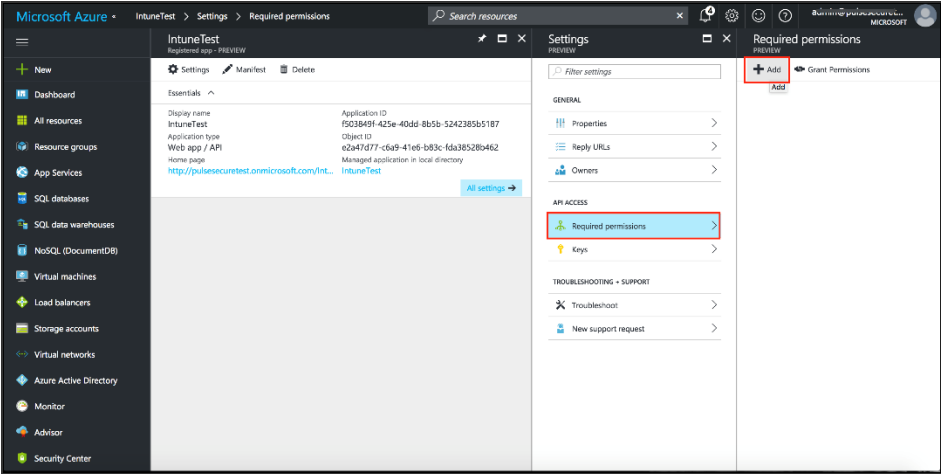
- 6. Enter the application name, select Web app/API as application type, and enter the IP address/FQDN for sign-on-URL and Click Create.



The Application Registration page appears if the registration is successful.

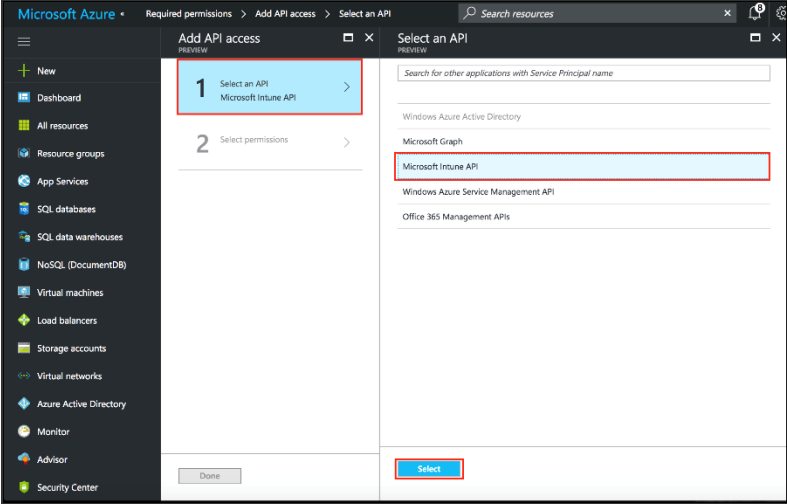


7. Click the application and select the required permissions and click **Add**.

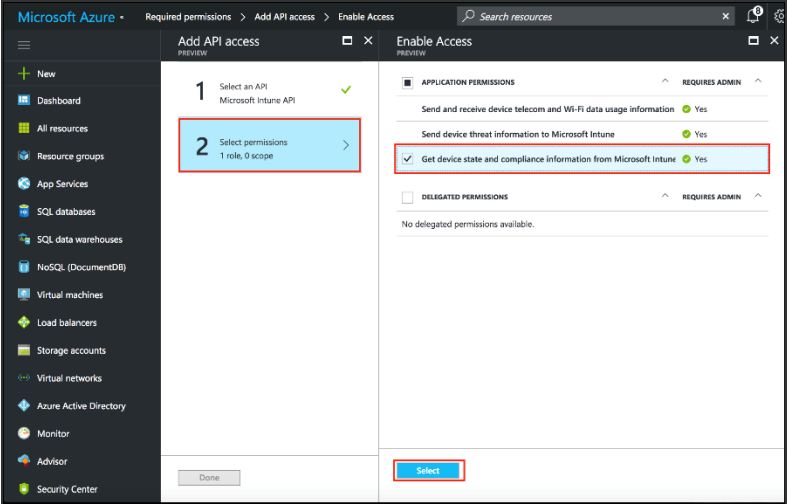


8. Click **Grant Permission**.

9. Select Microsoft Intune API.



Under Application Permissions, select Get device and compliance information from Microsoft Intune.

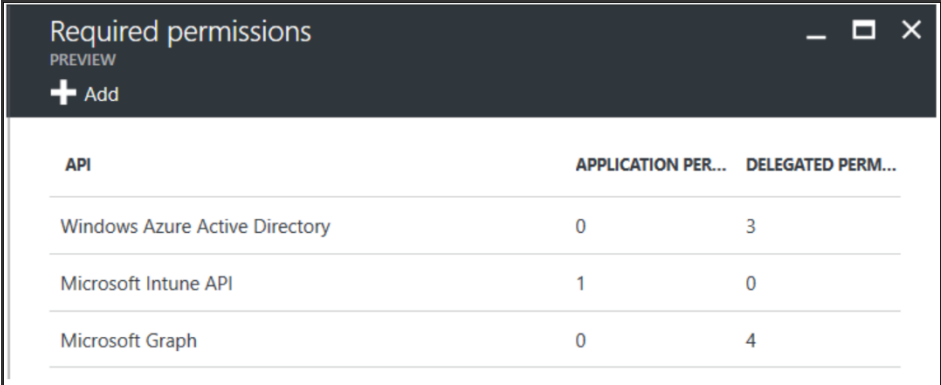


10. (Optional) You must add the following delegated permissions for Microsoft Graph API.

- Sign in and read user profile
- Sign Users in
- View users' email address
- View users' basic profile

11. (Optional) Add the following delegated permissions for Azure Active Directory.

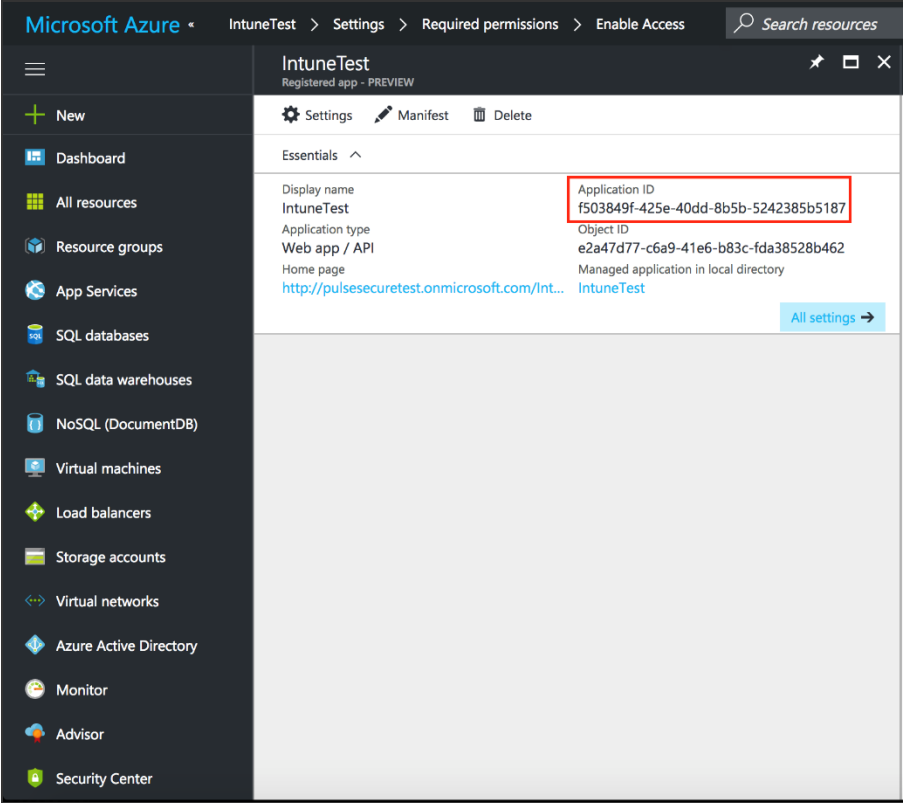
- Sign in and read user profile
- Read all users' basic profiles
- Access the directory as the signed-in user.



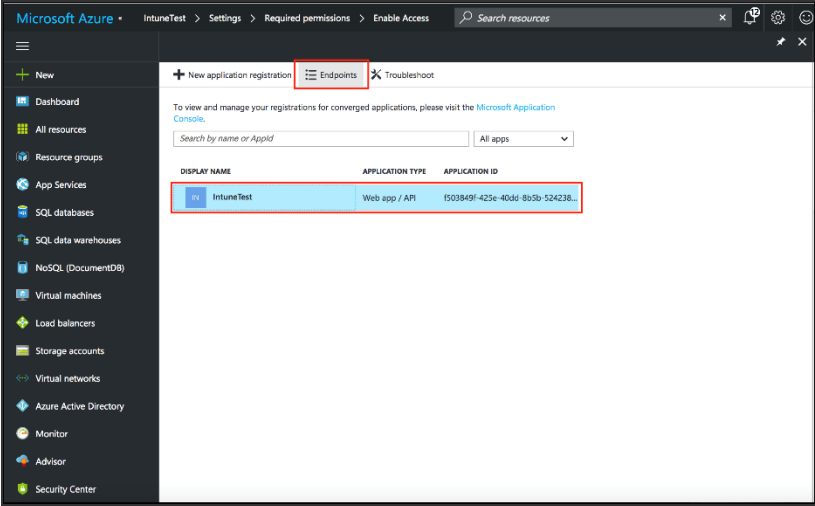
API	APPLICATION PER...	DELEGATED PERM...
Windows Azure Active Directory	0	3
Microsoft Intune API	1	0
Microsoft Graph	0	4

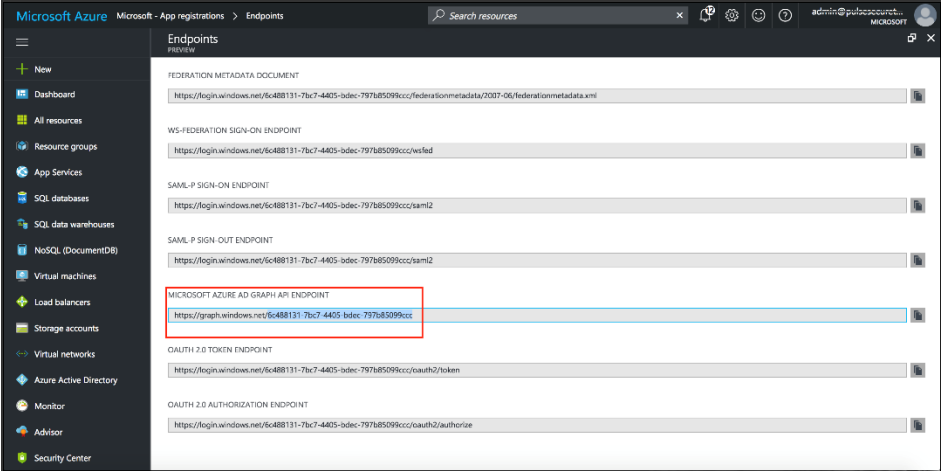
Viewing Client ID, Tenant ID, and Client Secret

The Client ID/Application ID is created automatically once the AAD web application/API is created. You can view the client ID/application ID from the application properties page.

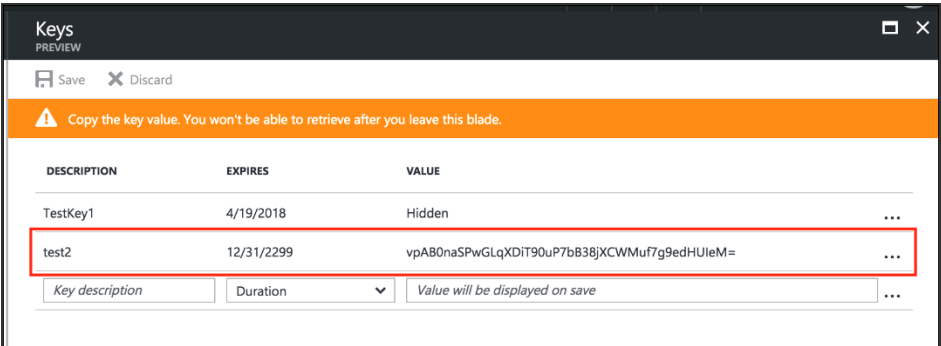
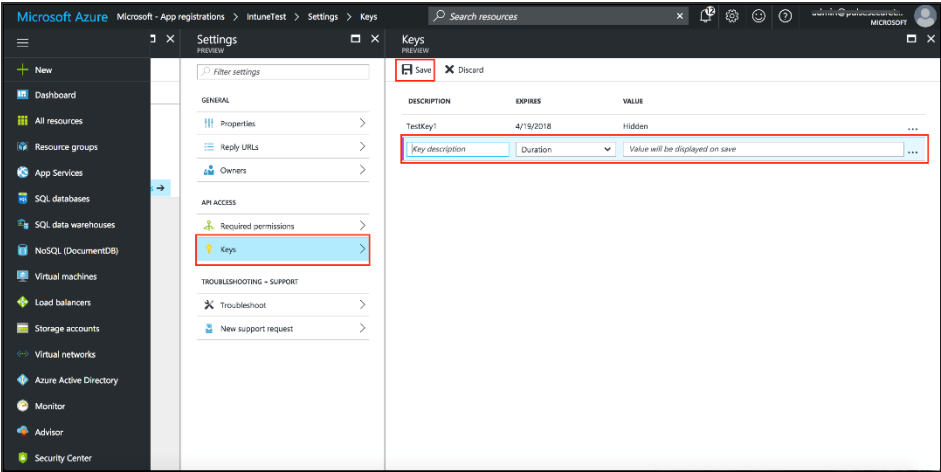


Every organization in Microsoft cloud is called tenant and it is organization specific. Each Tenant will be having a unique Tenant ID. Select the web application/API and click Endpoints tab and then you can copy the tenant ID.





To create the secret key, click the Web Application/API and then click Keys.



Configuring the PWS MDM

Pulse Workspace acts as the Mobile Device Management (MDM) Server for IPS solution. IPS users have to register their mobile devices with Pulse Workspace. As part of registration, the relevant Profiles get automatically provisioned to mobile device.

To configure the PWS MDM:

1. Enroll the devices in the MDM.
2. Create an enterprise WiFi profile. For more information, see Enterprise WiFi configuration
3. Configure IPS with a role and realm for the user using the Certificate authentication server. PWS provides the user with a link to provision the created policy and then pushes the profile information. IPS does the role assignment and either allows or denies based on the device assessment. For more information, see Configuring IPS.

Configuring the AirWatch MDM

To configure the AirWatch MDM:

1. Enroll devices in the MDM using the methods supported by the MDM.
2. Create a profile with the following MDM management options:
 - Certificate template- Create a configuration that specifies the field and type of identifier for client device certificates.
The MDM configuration templates provide flexibility in how the device identifier can be placed in the device certificate's subject or alternative subject. We recommend you include the user ID in the certificate, so the certificate can identify both the user and the device. For example:
CN= <EnrollmentUser>, serialNumber= <DeviceUid>, o=Company
 - Credential profile- Create a configuration that specifies the certificate authority and certificate template configuration.
 - Wi-Fi profile- Create a configuration that specifies the SSID, security options, and the credential configuration.
3. Save and deploy the profile to devices registered with your organization.
4. Enable API access and generate the AirWatch API key (tenant code).

The tenant code is part of the REST API configuration. The tenant code must be included in IPS MDM server configuration.

Certificate Template - Add / Edit

Name*

Description

Certificate Authority*

Issuing Template

Subject Name*

Private Key Length*

Private Key Type* Signing Encryption

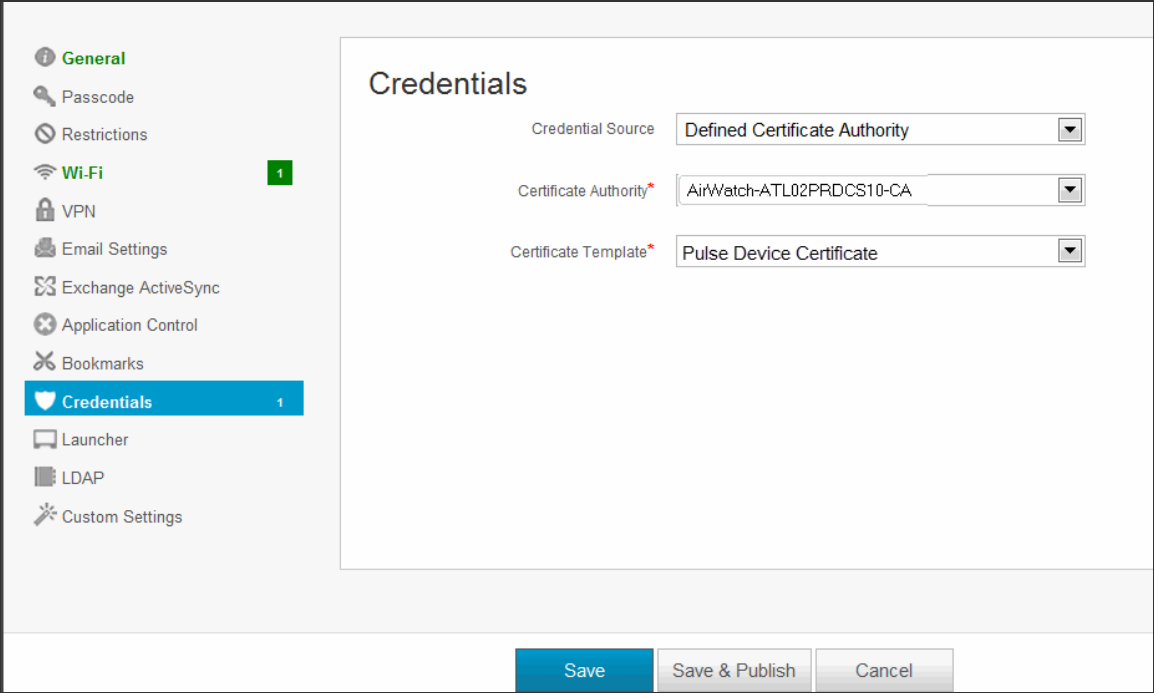
San Type Add

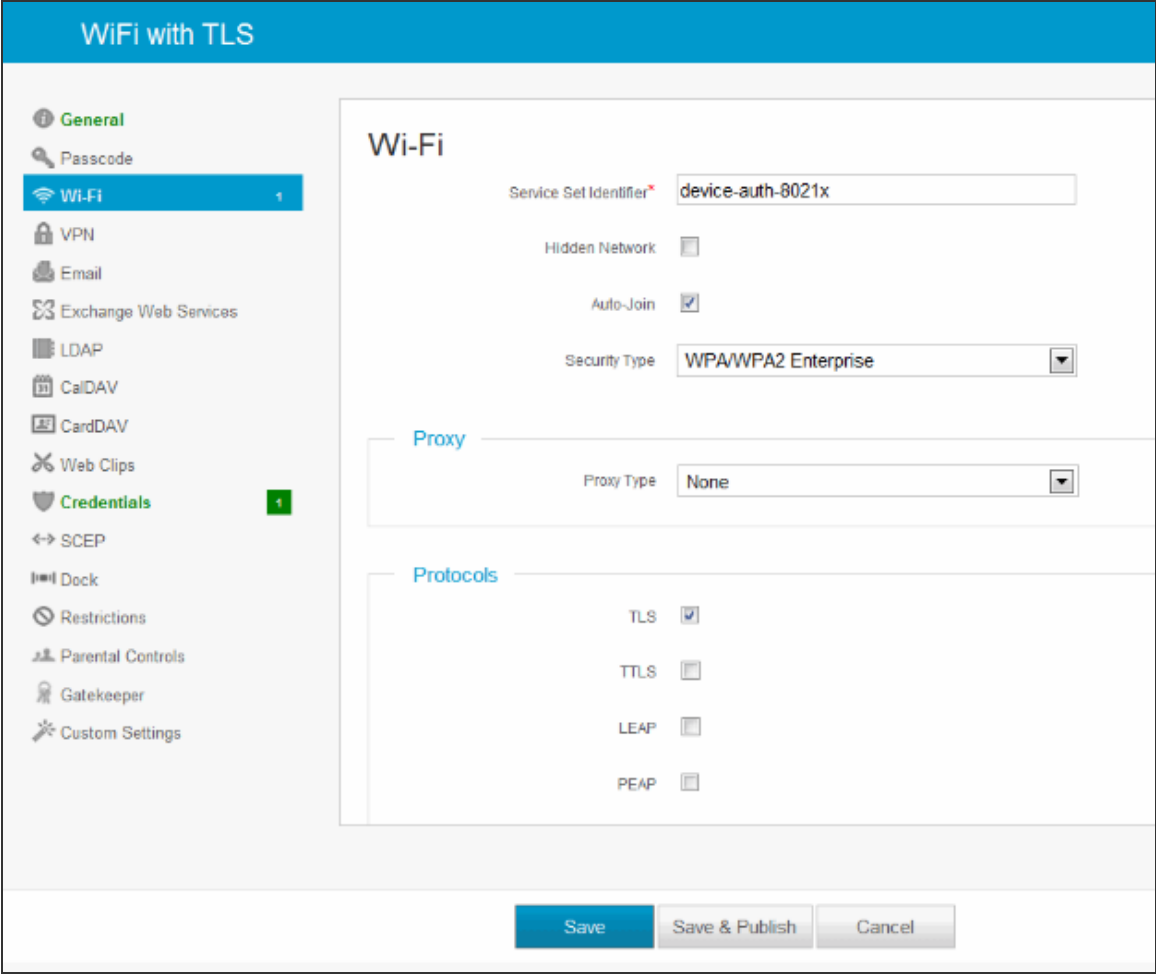
Automatic Certificate Renewal

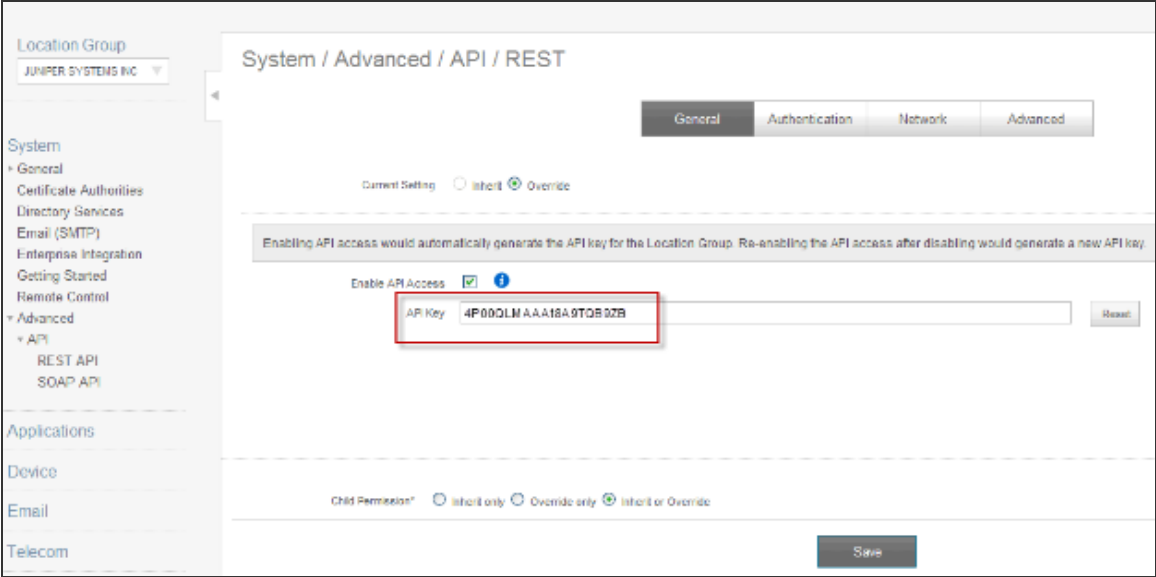
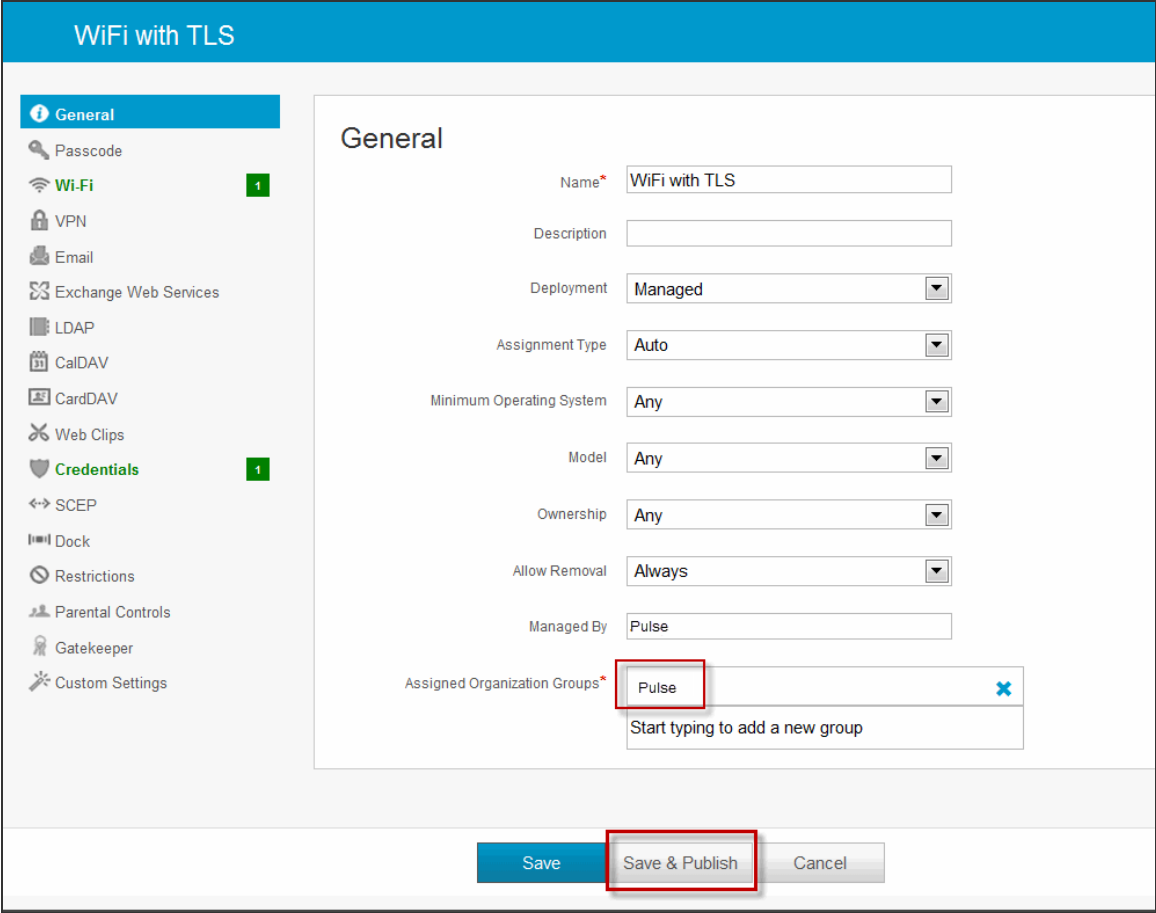
Auto Renewal Period (days)*

Enable Certificate Revocation

Publish Private Key







Configuring the MobileIron MDM

To configure the MobileIron MDM:

1. Enroll devices in the MDM using the methods supported by the MDM.
2. Create a Simple Certificate Enrollment Protocol (SCEP) configuration that specifies the field and type of identifier for client device certificates.
The MDM configuration templates provide flexibility in how the device identifier can be placed in the device certificate's subject or alternative subject. We recommend you include the user ID in the certificate, so the certificate can identify both the user and the device. For example:
CN=<DEVICE_UUID>, uid=<USER_ID>, o=Company
3. Create a Wi-Fi configuration that specifies the SSID and security options. During the enrollment process, this profile is provisioned to the device. Select the SCEP configuration completed in Step 2.
4. Select the Wi-Fi Profile configuration and apply it to a group label you have provisioned to manage this group of devices.



Wi-Fi connect fails if it is configured to use a device certificate that is signed by an intermediate CA and selects this in Wi-Fi profile trusted CA. Root CA has to be selected to properly work.

5. Apply the group label to the devices when you add them to the MDM. If they have already been added to the MDM, use the edit configuration utilities in the device inventory page to apply the group label.

New Wifi Setting

Name: Pulse Secure Access

Network Name (SSID): device-auth-802d

Description:

Hidden Network:

Authentication: WPA2 Enterprise

Data Encryption: AES

User Name: \$USERID\$

Password: \$PASSWORD\$

Apply to Certificates: Available

- System - iOS Enrollment CA Certificate
- sumitclientauth
- System - iOS MDM CA Certificate
- new

Selected:

Trusted Certificate Names: (Note: Enter comma (,) separated certificate names for multiple authentication servers.)

Allow Trust Exceptions:

Use Per-connection Password:

EAP Type: EAP-FAST EAP-SIM LEAP PEAP TLS TTLS

Identity Certificate: Pulse Device Certificate

Save Cancel

Microsoft Azure - App registrations

Microsoft - App registrations

Search resources

Search (Ctrl+F)

+ New application registration

Endpoints Troubleshoot

New application registration

To view and manage your registrations for converged applications, please visit the [Microsoft Application Console](#).

Search by name or AppId All apps

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
--------------	------------------	----------------

MobileIron ADMIN PORTAL

USERS & DEVICES APPS POLICIES & CONFIGS SETTINGS LOGS & EVENTS

Dashboard Devices ActiveSync Associations Labels Users Retired Devices

Actions + Add Labels: All-Smartphones Search by User or Device Advanced Search Pending Device Report

User	Phone	OS	Country	Status	Registered on Date	Last Check-In	E/C	Open
Pulse	Galaxy Nexus by sams...	Android 4.2		Active	2013-07-12	33 d 2 h	C	
Pulse TME	+14084315645 iPhone 4	iOS 6.1	United States	Active	2013-07-10	20 d 2 h	C	AT&
Pulse TME	PDA 6 iPad, 3rd gen	iOS 6.1	United States	Active	2013-07-15	55 m 39 s	C	AT&

Troubleshooting

During initial configuration, enable event logs for MDM API calls. You can use these logs to verify proper configuration. After you have verified proper configuration, you can disable logging for these events. Then, enable only for troubleshooting.

To enable logging for MDM API calls:

1. Select **System Log/Monitoring**.
2. Click the **Events** tab.
3. Click the **Settings** tab to display the configuration page.

After you have completed the MDM server configuration, you can view system event logs to verify that the polling is occurring.

To display the Events log:

1. Select **System Log/Monitoring**.
2. Click the **Events** tab.
3. Click the **Log** tab.

Next, to verify user access, you can attempt to connect to a wireless access point with your smart phone, and then view the user access logs.

To display the User Access log:

1. Select **System Log/Monitoring**.
2. Click the **User Access** tab.
3. Click the **Log** tab.

After you have verified proper configuration, you are not likely to need to tune the authentication server configuration, the 802.1x framework, or the enforcement points. However, based on user experience, MDM capabilities, and security threats, there are a few configuration elements you might want to tune from time to time.

Table describes these configuration elements.

Configuration Element	Tuning
Remediation	<p>In a network access control solution, noncompliant endpoints are typically placed in a remediation VLAN that serves a Web page. The Web page explains the steps users can take to make their endpoints compliant so that they can access the network.</p> <p>Your reasons for denying access might change from time to time. For example, your initial policy might be based on compliance with an MDM policy, and you can give steps on how to bring a device into compliance. You want to set an expectation on how long it takes for the MDM to reassess compliance. You might want to factor in IPS device check interval to estimate how long until the device can access the network.</p> <p>When there are new threats that exploit vulnerabilities in specific mobile platforms, you might create rules on the fly that deny access from specific platforms. If events like this occur, you might want to update your remediation message so that users can understand why access is denied.</p>
Realm – Device Check Interval	<p>You might want to tune this setting as you learn how frequently the MDM updates device records, or if the standard practice of the MDM changes. If the MDM records are updated every four hours, it does not make sense to poll every 10 minutes. If the MDM records are updated in real time, it might make sense to poll every 10 minutes.</p>
Roles and role mapping rules	<p>As you learn about mobile security threats and vulnerabilities, you might make changes to roles and role mapping rules or create new classifications. In general, you list restrictive rules first and set the stop flag. For example, if a device is noncompliant and maps to a noncompliant role, you would list it near the top of the rules for the realm and set the stop flag.</p> <p>Classification based on device type or platform can be more complicated. When you initially role out your BYOD solution, you might want to use roles to merely classify the devices, and so the rule classifying it would not need to be near the top of the list and would not need to have a stop flag. In response to a threat, however, you might want to use the role and role mapping configuration to deny access from a specific device platform. If events like this occur, you can edit your rules to map the vulnerable platform to an appropriate role and set the stop flag so that permissive roles are not assigned.</p>

Configuration Element	Tuning
RADIUS return attribute policy	Likewise, in response to threats and vulnerabilities, you can edit your rules to place formerly trusted device types into a remediation or guest VLAN instead of an employee VLAN; and then allow access again when you are no longer concerned with the threat.
Infranet Enforcer resource access policy	Likewise, in response to threats and vulnerabilities, you can edit your rules to deny access from formerly trusted device types; and then allow access again when you are no longer concerned with the threat.

Using the Debug Logs

The Ivanti Global Support Center might direct you to create a debug log to assist them in helping you debug an issue with the system. The debug log is used only by PSGSC.

To use debug logging:

1. Select **Troubleshooting > Monitoring > Debug Log** to display the configuration page. Complete the configuration as described in table below.
2. Click Save Changes. When you save changes with **Debug Logging On** selected, the system begins generating debug log entries.
3. Initiate the action you want to debug, such as a user sign in. You can reset the debug log file to restart debug logging if it takes you too long to initiate the action.
4. Click **Save Debug Log** to save the debug log to a file that you can send to PSGSC. You can clear the log after you have saved it to a file.
5. Clear the Debug Logging On check box and click **Save Changes** to turn off debug logging.

Settings	Guidelines
Current Log Size	Displays the size of the current log file. If it is large, use the controls to save, reset, or clear the log file.
Debug Logging On	Select to turn on debug logging.

Settings	Guidelines
Debug Log Size	Specify a maximum debug logfile size. The default is 2 MB. The maximum is 250 MB.
Debug Log Detail Level	Specify the debug log detail level. Obtain this from PSGSC.
Include logs	Select this option to include system logs in the debug log file. Recommended.
Process Names	Specify the process name. Obtain this from PSGSC.
Event Codes	Specify the event code. Obtain this from PSGSC. For MDM integration issues, PSGSC typically likes to collect debugging information for codes MDM, Auth, agentman, and Realm. The text is not case sensitive.

AAA Servers

AAA Server Overview

Overview

AAA stands for authentication, authorization, and accounting. An AAA server is a database that stores user credentials—username and password—and, in some cases, group information or other user attributes. The authentication results and group or user attribute information are used by Pulse Secure access management framework policy for decisions.

In the Pulse Secure access management framework, the sign-in page, realm, and AAA server configurations are associated. They determine user access and user role. A user submits credentials through a sign-in page, which specifies a realm, which is associated with a AAA server. If the access request meets the realm's authentication policy, the system forwards the user's credentials to the associated authentication server. The authentication server's job is to verify the user's identity. After verifying the user, the authentication server sends approval. If the realm also uses the server as a directory/attribute server, the AAA server sends the user's group information or other user attribute information. The access management framework then evaluates the realm's role-mapping rules to determine the user roles that apply to the session.

The Pulse Secure access management framework supports the following types of AAA servers:

- **Local**—You can create special purpose local databases to manually create user accounts, manage guest user access, permit anonymous access, or manage access based on digital certificates or MAC addresses.
- **External (standards-based)**—You can integrate standards-based LDAP and RADIUS servers with the access management framework. In addition to using the backend server for authentication, you can use LDAP group and RADIUS attribute information in role-mapping rules.
- **External (other)**—You can integrate compatible versions of popular third-party AAA servers with the access management framework. In addition to using the backend server for authentication, you can use Active Directory group information and SiteMinder attributes in role-mapping rules. In addition, you can use MDM device attributes in role mapping rules.

The following table is a reference of the AAA servers supported in IPS deployments.

	IPS
Local	Local Authentication Server Overview Anonymous Server Overview Certificate Server Overview MAC Address Authentication Server Overview *Special features to manage guest users.
External (standards-based)	LDAP Server Overview RADIUS Server Overview
External (other)	Active Directory Feature Support NIS Server Overview RSA Authentication Manager Overview SiteMinder Server Overview SQL Auth Server Overview

Authentication Protocols Used by AAA Servers

Policy Secure supports multiple authentication protocols. The following authentication servers require the protocols listed:

- **Local authentication servers**—If the passwords are stored as hashed values, the protocols available are PAP and MS-CHAP v1 with or without EAP. If the passwords are stored as clear text, CHAP and MD5-Challenge are also available.
- **Active directory**—The protocols available for inner authentication are PAP, MSCHAP and MS-CHAP v2, with or without EAP.
- **LDAP**—CHAP, EAP-MD5-Challenge, MS-CHAP v1, and MS-CHAP v2 protocols can be used with an LDAP authentication server only if the administration password is in clear text. By default, challenge response protocols are disabled for LDAP servers. Use these protocols only with noninteractive devices (for example, phones), as password management is not possible if these protocols are used for authentication.
- **Anonymous authentication server**—The anonymous authentication server is not supported with the open protocols.

AAA Traffic Management

From 9.0R3 release, the IPS Virtual appliances and the Physical Appliances allow the administrator to choose the communicating interface or the network for each authentication server.

This feature allows the AAA traffic across the following interfaces:

- Physical internal
- Physical external
- Physical management
- Virtual ports for physical interfaces
- VLAN ports
- Virtual ports on VLAN interfaces

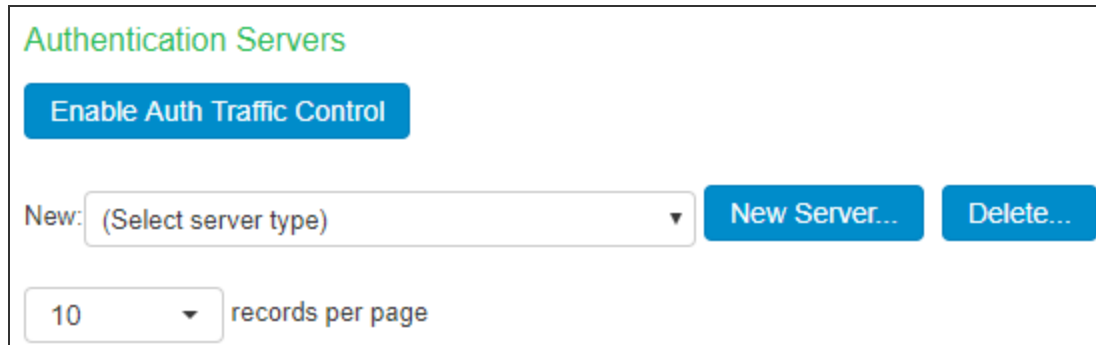
This feature allows to connect to remote supported authentication servers through any interfaces based on the network topology.

The following Authentication server types are supported:

- LDAP
- Active Directory
- RADIUS
- SiteMinder

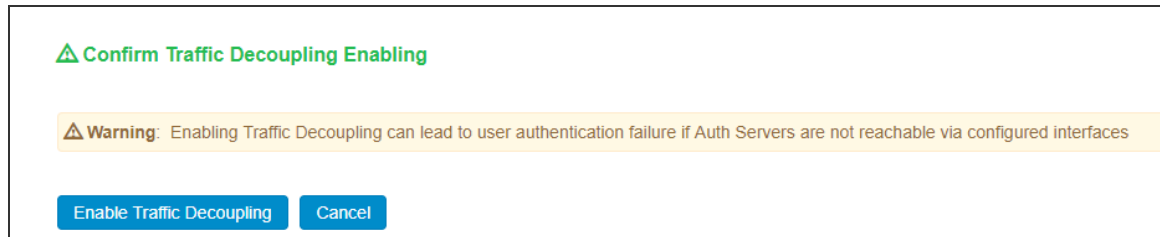
Configuring AAA Traffic Management Across Interfaces

1. Select **Authentication** > **Auth Servers** and configure service provider AAA configurations as needed.



The screenshot shows the 'Authentication Servers' configuration page. At the top, there is a green heading 'Authentication Servers'. Below it is a blue button labeled 'Enable Auth Traffic Control'. Underneath, there is a 'New:' dropdown menu with '(Select server type)' as the selected option. To the right of the dropdown are two blue buttons: 'New Server...' and 'Delete...'. At the bottom of the page, there is a dropdown menu showing '10' and the text 'records per page'.

2. Click **Enable Auth Traffic Control**. A new window appears.



The screenshot shows a dialog box titled 'Confirm Traffic Decoupling Enabling'. At the top, there is a green warning icon and the title. Below the title is a yellow warning box with a triangle icon and the text: 'Warning: Enabling Traffic Decoupling can lead to user authentication failure if Auth Servers are not reachable via configured interfaces'. At the bottom of the dialog, there are two blue buttons: 'Enable Traffic Decoupling' and 'Cancel'.

3. Click **Enable Traffic Decoupling** to confirm. The page navigates to the Auth server page that displays the options to configure the AAA traffic interfaces.



For external port, it enables the external port to respond to incoming RADIUS client requests on the external port as well as communicate with authentication servers through that port.

Authentication Servers

▼ NIC Selection

Global Setting Auth Server Level

Chose the interface from the below list for reaching to Auth Server

localhost2 Management

4. Select **Global setting** to use same interface across all supported authentication servers or select **Auth Server Level** to select the interface for a specific authentication server for the AAA traffic.

Authentication Servers

Traffic Decoupling Enabled

NIC Selection

Global Setting Auth Server Level
Chose the interface from the below list for reaching to Auth Server

PPS_102 Internal internal 10.204.88.102
PPS_101 Internal internal 10.204.88.101

Save Disable Auth Traffic Control

New: (Select server type) New Server... Delete...

10 records per page Search:

<input checked="" type="checkbox"/>	Authentication/Authorization Servers	Type
<input type="checkbox"/>	Administrators	Local Authentication
<input type="checkbox"/>	Certificate Authentication	Certificate Server
<input type="checkbox"/>	Guest Authentication	Local Authentication
<input type="checkbox"/>	Guest Wired Authentication	MAC Address Authentication
<input type="checkbox"/>	Local Profiler-1	Local Profiler
<input type="checkbox"/>	System Local	Local Authentication

Authentication Servers

Port Selection

Global Setting Auth Server Level
Supported Auth Servers: Active Directory, LDAP, RADIUS, Site-Minder

Save Disable Auth Traffic Control

New: (Select server type) New Server... Delete...

10 records per page Search:

<input checked="" type="checkbox"/>	Authentication/Authorization Servers	Type
<input type="checkbox"/>	Administrators	Local Authentication
<input type="checkbox"/>	AD-LDAP-SRV	LDAP Server
<input type="checkbox"/>	AD-SERVER	Active Directory / Windows NT
<input type="checkbox"/>	Certificate Authentication	Certificate Server
<input type="checkbox"/>	Guest Authentication	Local Authentication
<input type="checkbox"/>	Guest Wired Authentication	MAC Address Authentication
<input type="checkbox"/>	RADIUS-SERVER	RADIUS Server
<input type="checkbox"/>	SiteMinder	SiteMinder Server
<input type="checkbox"/>	SQL-SERVER	SQL Auth Server
<input type="checkbox"/>	System Local	Local Authentication

- Select the required interface and port from the list.
For Clusters, select applicable interfaces and associated ports.

Auth Servers > AD-SERVER > Settings

Settings

Settings Users Troubleshooting

▼ Base Configuration

* Name: Label to reference this server

* Domain: NetBIOS name of the domain

* Kerberos Realm: Specifies the Kerberos realm of the Active Directory domain. It is usually set to the DNS name of the Active Directory domain. Example "xyz.net", "abc.com"

▼ Port Selection

Set the port for reaching to Auth Server

PPS-129-PRI

PPS-123-SEC

- Click **Save**.

AAA Server Configuration Task Summary

To integrate an authentication server:

- Configure the authentication server. Select **Authentication > Auth. Servers page** and complete the authentication server configuration.
- Create an authentication realm. Select **Users > User Realms** or **Administrators > Admin Realms** and select the authentication server when you complete the authentication realm configuration.

Using the Local Authentication Server

This topic describes the local authentication server.

Local Authentication Server Overview

The local authentication server is an authentication database that is built in to IPS. Therefore, it is considered a "local" server in contrast to a third-party enterprise AAA server that is connected over the network.

Typically, you create local user accounts for temporary users who do not have accounts on your enterprise AAA servers. Temporary users include lab users or guests, but you might find the local authentication server useful to create temporary accounts for users who are normally verified by an enterprise AAA server that you plan to disable.

You also use the local authentication server to create accounts for administrator users, such as system administrators and guest user access managers (GUAM).



Although it is common practice to use the local authentication server for administrator accounts, it does not preclude you from using any of the supported third-party enterprise AAA servers in your administrator access management framework.

The following authentication protocol sets can be used with the local authentication server:

- By default, the system uses hashing to store passwords. When using the default, the protocols available are PAP and MS-CHAP v1 with or without EAP.
- You can enable an option to store passwords as clear text. If you enable this option, CHAP and MD5-Challenge are also available.

Configuring the Local Authentication Server

You can create multiple local authentication server instances. When you define a new local authentication server, you must give the server a unique name and configure options for passwords and guest users.

To create a local authentication server:

1. Select **Authentication > Auth. Servers**.
2. Select **Local Authentication** and click **New Server** to display the configuration page.
3. The Local Authentication Server configuration page.
4. Complete the configuration as described in table.
5. Save the configuration.

Auth Servers > New Local Authentication

New Local Authentication

*Name: Local Auth Label to reference this server.

▼ Password Options

Minimum length: 10 characters
 Maximum length: 128 characters

Password must have at least 1 digits
 Password must have at least 1 letters
 Password must have mix of UPPERCASE and lowercase letters
 Password must be different from username
 New passwords must be different from previous password

Password Storage Type

Strong Hash
Note: Highly secure, but not compatible with some of the authentication protocols i.e. CHAP, EAP-MD5 and MS-CHAP (V1/V2)

Legacy Hash This option can only be set during create
Note: Compatible with MSCHAP(v1/V2) although less secure

Clear Text This option can only be set during create
Note: Compatible with all authentication protocols i.e. CHAP, EAP-MD5, MSCHAP(v1/V2) although not secure

▼ Password Management

Allow users to change their passwords

Force password change after 1 days
 Prompt users to change their password 1 days before current password expires

Note: Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities

▼ Account Lockout

Enable Account Lockout for users

Maximum wrong password attempts: 3 (3 and above)
 Account Lockout period (minutes): 10 (10 and above)

▼ Guest Access

Guest User Account Managers

Enable Guest User Account Managers to administer Guest Accounts Configure system GUAM settings

Instructions for Guest User Account Manager: Instructions displayed for guest users creation and updation. You can use ,
, , <noscript>, and tags to format the text.

Maximum Account Validity Period: 24 Set the Guest Account length limit (end time minus start time) in hours. This is valid for guests created by Guest Admin. Does not impact existing user expirations.

Guest Self-Registration

Send guest user credentials via: SMS Email Configure SMS/Email settings

Show credentials on screen after guest completes registration
 Enable Sponsored Guest Access
 Maximum Account Validity Period for Self Registered Guests: 24 Set the Guest Account length limit in hours. This is valid for self registered guests. Does not impact existing user expirations.

Note: To enable Guest Self-Registration navigate to Signing In > Sign-in Policies > User URLs > [url] > Configure Guest Settings

Common configuration for Guest User Account Managers and Guest Self-Registration

Guest User Name Prefix: guest_ Prefix applied to auto-generated user names.

Guest User Info Fields: Enter additional fields for guest user information, one field per line. For example:



Company Name
 Host or Sponsor
 Title
 Company name
 Sponsor



▼ Server Catalog

To Enable Attribute Editing, please save Local Server Configuration.

* indicates required field

Settings	Guidelines
Name	Specify a name that is useful to you.

Settings	Guidelines
Password Options	
Minimum length	Specify a number of characters. The valid range is 0-99. 6 is the default.
Maximum length	Specify a number of characters. The valid range is 0-99. 8 is the default. The maximum length cannot be less than the minimum length.
Minimum digits	Specify the number of digits required in a password. Do not require more digits than the value of the maximum length option.
Minimum letters	Specify the number of letters required in a password. Do not require more letters than the value of the maximum length option. If you enable the previous option, the combined total of the two options cannot exceed that of the value specified in the maximum length option.
Uppercase and lowercase required	<p>Select this option if you want all passwords to contain a mixture of uppercase and lowercase letters.</p> <hr/> <p> Require passwords to contain at least two letters if you also require a mix of uppercase and lowercase letters.</p> <hr/>
Different from username	Select this option if the password cannot equal the username.
Different from previous password	Select this option if a new password cannot equal the previous password.
Password Storage Hash	
Strong Hash	<p>Select this option to protect passwords using stronger hash algorithm for high security.</p> <hr/> <p> This option is not compatible with some of the protocols such as CHAP, EAP-MD5 and MS-CHAP (V1/V2). For Native Supplicant this option is supported only with PAP protocol.</p> <hr/> <p>On upgrading IPS from previous version to 9.1R4 version there is no change in the password storage type and all the local authentication servers from previous release will be moved to newer release with same password storage type. After upgrading IPS to newer version, administrator has an option to switch to Strong hash if the previous password storage type is Legacy hash.</p>

Settings	Guidelines
	<ul style="list-style-type: none"> • After switching to strong hash, all the existing users still use the legacy hash as password. To migrate to strong hash, users need to reset their password. • After switching to strong hash, any new users created will use strong hash for the password.
Legacy Hash	Select this option to protect passwords using MS-CHAP (V1/V2).
Clear text	<p>Select this option if you are using open authentication protocol sets. CHAP and EAP-MD5-Challenge work with local authentication servers only if you select this option.</p> <hr/> <p> Be aware of the security implications of storing passwords as clear text.</p> <hr/>
Password Management	
Allow users to change passwords	<p>Select this option if you want users to be able to change their passwords.</p> <hr/> <p> In addition to selecting local authentication password management options, you must select the Enable Password Management option for the associated realm authentication policy.</p> <hr/>
Force password change	Select this option to specify the number of days after which a password expires. The default is 64 days.
Prompt users to change password	Select this option to specify when to prompt the user to change passwords.
Guest Access Configurations	
Enable Guest User Account Managers	<p>Select this option to allow guest user account managers to create guest user accounts on the local authentication server.</p> <p>In some businesses, you might want to delegate responsibility for temporary or guest users to a guest user access manager (GUAM) who can use the local authentication server to provision accounts for guests.</p>
Guest User Name Prefix	<p>Specify the prefix to be used in auto generated guest usernames.</p> <p>We recommend you retain the default guest_ so that you can rely on the naming convention in your role mapping rules.</p>

Settings	Guidelines
Guest User Info Fields	(Optional) Add line items to represent fields that you want to appear on the configuration page for creating guest user accounts. For example, you can create fields for Company Name, Host Person, Meal Preference, and so on.
Instructions for Guest User Account Manager	(Optional) Add instructions to the GUAM that appear on the GUAM sign-in page. You can use the following HTML tags to format the text: , , , <noscript>, and <a href>.
Maximum Account Validity Period	Specify the number of hours the account is valid. The default is 12 hours.
Server Catalog	
Attributes	The Attributes button appears after you have saved the server information. Click the Attributes button to display the server catalog. Configure the attribute value.

Defining Framed-IP Address

The Framed-IP attribute can be used in usecases, such as Access Point Name (APN), which manages the modems in broadband service provider network.

APN is added as a RADIUS client and it can authenticate the modem MAC addresses with Ivanti Policy Secure and assign IP Addresses associated with respective IP address configured on IPS.

To define Framed-IP attribute:

1. Select **Authentication > Auth.Servers** and select the local authentication server.
2. Under Server Catalog, Click **Attributes** and create the attributes. For example, IP Address.
3. Navigate to the users page, create new user and set attribute values.
4. Navigate to **Endpoint > Network Access > Radius Attributes > RADIUS Return Attributes**.
5. Set the Auth Server Catalog Attribute Value (userAttr.Framed-IP).
6. Click **Save Changes**.

The screenshot shows the 'Guest Self-Registration' configuration page. A modal dialog titled 'Attributes' is open, displaying a list of attributes. The 'IP Address' attribute is selected. The dialog also shows a 'Save Changes' button and a list of other attributes like 'employeeType', 'enable', 'homeDirectory', 'homeDrive', 'o', 'one time use', and 'ou'. The background page shows options for sending credentials via SMS or Email, and a section for common configuration for Guest User Account Managers and Guest User Info Fields.

The screenshot shows the 'Control the Access' configuration page. It includes a table for Return Attributes with columns for Return Attribute, Radius Auth Server Attribute Value, Auth Server Catalog Attribute Value, and Value. The table contains three rows: Filter-Id, Framed-IP-Address, and Framed-IP-Netmask.

Return Attribute	Radius Auth Server Attribute Value	Auth Server Catalog Attribute Value	Value
Filter-Id	-none-	-none-	
Framed-IP-Address	-none-	IP Address	
Framed-IP-Netmask	-none-	subnet mask	

Creating User Accounts

You use the Users page to create local authentication server user accounts. A user account includes a username and password to be used for authentication, as well as other information used for records and account management.

To create a local user account:

1. Select **Authentication > Auth. Servers**.
2. Select the local authentication server to which you want to add a user account.
3. Click the **Users** tab.
4. Click **New** to display the configuration page.
5. Complete the configuration as described in table.
6. Save the configuration.

Auth Servers > Demo-Local-Auth-Server > Users > Update Local User demouser

Update Local User demouser

Full Name:

Authenticate using: Demo-Local-Auth-Server

Password:

Confirm Password:

Start Time:

End Time:

Time Zone: (GMT+05:30) Kolkata, Chennai, Mumbai, New Delhi

Company Name


Host or Sponsor


One-time use (disable account after the next successful sign-in)
 Enabled
 Disabled
 Quarantined
 Require user to change password at next sign in

Note: You must also configure password management on the Authentication server Settings with 'Allow users to change their passwords' option enabled. Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities.

▼ Custom Attributes

Attribute	Value	
<input type="text" value="-none-"/>	<input type="text"/>	<input type="button" value="Add"/>
<input type="checkbox"/> Session-Timeout	120	
<input type="checkbox"/> Termination-Action	1	
<input type="checkbox"/> demo-custom-attribute	fill	

Settings	Guidelines
Username	Do not include “~” in a username.  You cannot change a username after you create the account.
Full Name	Specify the user’s full name.
Password	Specify a password. Make sure that the password you enter conforms to the password options specified on the local authentication server configuration page.
Confirm password	Confirm the password.

Settings	Guidelines
Start Time	(Optional) Specify a start and end time for the account. The system process that deletes expired user accounts runs every 10 minutes. There might be a delay of some minutes before the account is purged. Even if the system time or date is moved ahead past the expiration time, the account could still be valid until the purge process runs.
End Time	One-time user accounts are not deleted by the purge process; they are deleted immediately after the user exits.
Company Name	(Optional) Specify the company with which the user is associated.
Host or Sponsor	(Optional) Specify the host or sponsor—for example, the person at your company who requested that you create the account.
One-time use	Select this option to limit the user to one log in. After one successful log in, the user's log in state is set to disabled, and the user receives an error message when attempting subsequent sign-ins. However, you can manually reset this option to allow the same user to log in again. If you do not select this option, the user account is subject to the specified start and end time for the account.
Enabled	Select this check box if it is not already selected. If the one-time use option has been implemented, this option is listed as Disabled after the user has logged in successfully. If a permanent or one-time user is logged in and you disable this option, the user is immediately logged out of the system and receives an error message.
Require user to change password	<u>Select this option to force users to change their passwords at the next log in.</u>  If you force the user to change passwords, you must also enable the local authentication password management options.
Custom Attributes	Select the custom attribute created and specify the value. Radius Return Attributes from the dictionaries is pre-populated to the Server Catalog of Local Auth server so that they are available under the custom attributes for a specific user.

Managing User Accounts

You use the Users page to list, modify, and delete local authentication server user accounts.

To manage a user account:

1. Select **Authentication > Auth. Servers**.
2. Click the link for the authentication server you want to manage.
3. Click the **Users** tab to display the user accounts table.

The user accounts table includes entries for the accounts that have been created. The Last Sign-in Statistic column shows the last successful sign-in date and time for each user, the user's IP address, and the agent or browser type and version.

Use the controls to search for users and manage user accounts:

1. To search for a specific user, enter a username in the Show users named box and click Update.



You can use an asterisk (*) as a wildcard, where * represents any number of zero or more characters. For example, to search for all usernames that contain the letters jo, enter *jo*. The search is case-sensitive. To display the entire list of accounts again, type * or delete the field's contents and click Update.

2. To limit the number of users displayed on the page, enter a number in the Show N users box and click Update.
3. To edit the user account configuration, click the link in the Username column to display the Update Local User Account page.
4. To terminate the user session and delete the account, select the box next to the user account record and click **Delete**.

i	Username	Name	Usertype	Last Sign-in Statistic		
				Date&Time	IPAddress	Agent
<input type="checkbox"/>	hc	Unspecified Name	Normal	2016/08/29 16:54:27	10.209.122.134	Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36
<input type="checkbox"/>	priya	Unspecified Name	Normal	2016/07/22 14:47:49		
<input type="checkbox"/>	sathya	Unspecified Name	Normal	2016/07/28 16:56:56	10.209.122.94	
<input type="checkbox"/>	shreya	Unspecified Name	Normal	2016/07/19 12:37:33	10.209.122.239	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
<input type="checkbox"/>	surendra	Unspecified Name	Normal	2016/08/11 11:27:38		
<input type="checkbox"/>	test	Unspecified Name	Normal	2016/08/31 18:02:51	10.204.90.240	Pulse-Secure/8.2.5.869 (Windows 7) Pulse/5.2.5.869
<input type="checkbox"/>	uacqa	Unspecified Name	Normal	2016/08/10 22:41:20		
<input type="checkbox"/>	yashu	Unspecified Name	Normal	2016/08/05 13:03:49		
<input type="checkbox"/>	yashuser	Unspecified Name	Normal	2016/07/28 14:46:41		

The following figure shows the user account configuration page. You can use this page to modify the account settings, or to disable or quarantine the account.

The screenshot shows the 'Update Local User' configuration page. The breadcrumb trail is 'Auth Servers > System Local > Update Local User hc'. The page title is 'Update Local User hc'. The form includes the following fields and options:

- Full Name: Unspecified Name
- Authenticate using System Local
- Password: [Redacted]
- Confirm Password: [Redacted]
- Start Time: [Redacted]
- End Time: [Redacted]
- Time Zone: (GMT+05:30) Kolkata, Chennai, Mumbai, New Delhi
- One-time use (disable account after the next successful sign-in):
- Enabled:
- Disabled:
- Quarantined:
- Require user to change password at next sign in:

A note at the bottom states: 'Note: You must also configure password management on the Authentication server Settings with 'Allow users to change their passwords' option enabled. Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities.'

A 'Save Changes' button is located at the bottom left.

Creating Administrator User Accounts

You use the Admin Users page to create accounts for local authentication server administrators. An administrator user can create, modify, and delete user accounts.

The admin users you create on the Admin Users page can view and manage all users that have been added to the local authentication server. In contrast, admin users you create by assigning the GUAM role capability can view and manage only the user accounts they created.

To create an administrator user account:

1. Select **Authentication > Auth. Servers**.
2. Click the link for the Guest Authentication Server you want to manage.
3. Click the **Admin Users** tab to display the configuration page.
4. Specify a username, select an authentication realm, and click **Add** to create the administrator user.
5. Save the configuration.

The screenshot shows the 'Admin Users' configuration page. The breadcrumb trail is 'Auth Servers > System Local'. The page title is 'System Local'. The navigation tabs are 'Settings', 'Users', and 'Admin Users' (which is highlighted). The page contains the following information:

- A 'User Admin' has some administrator capabilities on the device, including adding new users, changing passwords, and deleting existing users. You can delegate these abilities to User Admins per authentication server.
- To create User Admins for server System Local, enter the user's username and the authentication realm used to authenticate the user. When this user signs in to the device, a "User Admin" link appears as a System menu. The user admin can click this link to manage users for the assigned authentication server.
- Note: Please double-check to make sure the username is spelled correctly before adding the User Admin to the list.
- An alternate option is to create a role for the "User Admin" which has the "Enable Guest User Account Management Rights" enabled. If using this role method, do not add a User Admin on this page. The advantage of the role option is that it will limit the "User Admin" to view only those accounts that they created.

The form includes the following fields and options:

- Add User Admin
- Username: [Redacted]
- Authentication Realm: Users
- Add -> button
- Remove button
- User Admins list: [Empty list]

Importing Users from CSV File

To bulk import users, or to add/change information about your users, you can use CSV Import feature.

Prepare a CSV for import. The mandatory required field's in the CSV is Username, password, you can choose to include additional user information if possible. View our available import fields and their associated formatting requirements in the CSV Import Fields table below.

1. Select **Auth Servers > System Local (Administrators, System Local, Guest Authentication) > Users**.
2. Click the **Browse** button to select the CSV file.
3. Enable Overwrite users to overwrite users with the same username if required. If the username exists in the local database before importing, enabling the overwrite option will delete the old entry and re-place with the newer entry present in the CSV file.

The CSV import allows you to import users in bulk with the following fields. Note that the header fields in your CSV must precisely match as shown in the CSV Fields column below in order for your import to be successful.

CSV Import Fields

CSV Fields	Description	Formatting Requirements	Character Limitations
Username	User name This is the mandatory field for a CSV import.	Username should be not present in the Local database. If the Overwrite option is enabled the users with the same name in the local database will be overwritten.	Username should not contain "~" character.
Password	Password of the user		

CSV Fields	Description	Formatting Requirements	Character Limitations
This is the mandatory field for a CSV import.	Password should be based on the settings done in the password management/options for the specific local Auth server.	Password field should be in plaintext format.	
Full Name	Full Name (Optional field)	Only ASCII characters are accepted.	
Start Time	Start time (Optional field)	MM/DD/YYYY HH:MM:SS AM/PM	n/a
End Time	End time (Optional field)	MM/DD/YYYY HH:MM:SS AM/PM	n/a
Time Zone	Time Zone (Optional field)	To see the sample TimeZones in IPS:	
Navigate to System > Status > Overview > Date and Time.			
If the time zone is not mentioned in the CSV file, the default IPS timezone is considered.			
Use this format (including parentheses): (GMT+12:00) Alaska			
One Time Use	(Optional field)		
Disables the account after the next successful sign-in.	Only Binary values are accepted		

CSV Fields	Description	Formatting Requirements	Character Limitations
	"Disable- 0		
	"Enable- 1		
Enabled	(Optional field)		
Enable/Disable the user ID.	Only Binary values are accepted.		
	"Disable- 0		
	"Enable- 1		
Change Password at next sign in	(Optional field)		
Option to change the password for next sign-in	Only Binary values are accepted.		
	"Disable- 0		
	"Enable- 1		

Using Active Directory

This topic describes integration with the Microsoft® Windows® platform Active Directory™ service.

Microsoft Windows Platform Active Directory Service Overview

This section describes support for using IPS with the Active Directory AAA service.

Understanding Active Directory

Active Directory is a directory service used in Windows domain networks. It is included in most Windows server operating systems. Enterprise servers that run Active Directory are called domain controllers. An Active Directory domain controller authenticates and authorizes users and computers in a Windows domain network.

When you use Active Directory as the authentication and authorization service for your Pulse Secure access management framework, users can sign in to IPS using the same username and password they use to access their Windows desktops. You can also use Active Directory group information in role mapping rules.

From 9.1R1 onwards, Active Directory Legacy Mode configuration will not be supported. If you have an existing Active Directory authentication server using Legacy Mode, first migrate to Standard Mode and then upgrade IPS. For the detailed migration procedure, refer [KB40430](#)

Active Directory Feature Support

Pulse Secure access management framework supports the following Active Directory features:

- Honors trust relationships in Active Directory and Windows NT environments.
- Supports Domain Local Groups, Domain Global Groups, and Universal Groups defined in the Active Directory forest.
- Supports use of Kerberos, NTLMv2, and NTLMv1 authentication protocols.
- Supports [user principal name \(UPN\)](#) format for usernames. This support is available for Web log in, IPS at Layer 3, and EAP-MS-CHAP v2.

Interoperability Requirements and Limitations

The following limitations apply to interoperability with Active Directory:

- The Pulse Secure access management framework uses Active Directory security groups, not distribution groups. Security groups allow you to use one type of group for not only assigning rights and permissions, but also as a distribution list for e-mail.
- Each Active Directory configuration you create for the Pulse Secure access management framework should use a different and unique machine account name.
- If the current Active Directory domain controller is not reachable, the user or machine authentication requests fail for a few seconds (less than 2 minutes) before attempting to authenticate users with another domain controller in the Active Directory domain.

- We do not support interoperability with Active Directory implementations that use the equal sign operator (=) in a group name, such as: "\=THIRD FLOOR GROUP". The Pulse Secure access management framework authentication process involves search operations that use the equal sign operator (=) when parsing server catalogs to retrieve group names, usernames and domain names, as well as user_SID and domain_SID values. You might encounter unexpected behavior that can affect normal processing of authentication services if a group name configured on your Active Directory server includes an equal sign operator (=).
- Active Directory versions Windows 2008, Windows 2012 R2 and later use a dynamic port range. The default start port is 49152 and the default end port is 65535. Therefore, if there is a firewall between the Ivanti service and the Active Directory Service, you must increase the remote procedure call (RPC) port range on the firewall. See [Microsoft Knowledge Base article 929851](#).
- The Ivanti password management feature, which enables users to change their Active Directory passwords through the Ivanti service Web server, is not supported for users of trusted domains that do not trust the domain specified in the Ivanti Active Directory configuration.
- UPN format for user log in is not supported for MS-CHAP v2.

Understanding the Active Directory Standard Configuration


Active Directory standard configuration supports interoperability with any version of Active Directory, and is the required configuration mode to support authentication using MS-CHAP v2 with Windows 2008 R2 Active Directory Service. Machine authentication, for example, uses MS-CHAP v2.


Configuring Authentication and Authorization with Active Directory Service (Standard Mode)


To configure integration with Active Directory Service (standard mode):

1. Select **Authentication > Auth. Servers**.
2. Select **Active Directory / Windows NT** and click **New Server** to display the configuration page.
3. Select **Active Directory mode** and complete the configuration as described in table.
4. Save the configuration.

Settings	Guidelines
Mode	
	Select one of the following modes: Active Directory —For recent versions of Windows Server. This table describes Active Directory mode.
Base Configuration	
Name	Specify a name to identify the server within the system.
Domain	Specify the NetBIOS domain name for the Active Directory domain. The system uses DNS to discover domain controllers in the Active Directory forest. It sends authentication requests to the domain controller at the closest site. Ensure that your DNS servers are configured to resolve the Active Directory domain controller fully qualified domain name (FQDN) and service (SRV) records.
Kerberos Realm	Specify the FQDN of the Active Directory domain. For example, if “pulsesecure” is the domain name (NetBIOS name), then pulsesecure.net is the Kerberos realm name.
Domain Join Configuration	
Username	Specify a username that has permission to join computers to the Active Directory domain. Use the “Delegate Control” workflow in Active Directory to assign the following user account permissions to the username or to a group to which the user belongs: <ul style="list-style-type: none"> • Write • Write All Properties • Change Password • Reset Password • Validate Write to DNS hostname • Read and write DNS host attributes • Delete Computer Objects

Settings	Guidelines
	<ul style="list-style-type: none"> • Create Computer Objects
Password	Specify the password for the special user.
Save Credentials	<p>If this setting is not enabled, the credentials entered will be destroyed after successfully joining the domain.</p> <p>This option is useful when managing clusters. For example, you might want to save the credentials for a cluster node you have yet to add. If you do not enable this option, you must manually enter the credentials when you add the new cluster node.</p>
Container Name	<p>Specify the container path in Active Directory in which to create the machine account. Changing this field triggers a domain rejoin action.</p> <p>The default is Computers, which is a standard container created during installation of the AD server. The AD Computers container is the default location for new computer accounts created in the domain.</p> <p>If desired, you may specify a different container or OU. To specify nested containers, use a forward slash (/) as the container separator. For example: outer OU/inner OU.</p> <hr/> <p> Do not use backslashes in the path. Using backslashes causes an Invalid DN Syntax error.</p> <hr/>
Computer Name	Specify the machine account name. The default computer name is derived from the license hardware in the following format: 0161MT2L00K2C0. We recommend the Computer Name string contain no more than 14 characters to avoid potential issues with the AD/NT server. Do not include the '\$' character.
Update Join Status / Reset Join	<p>The following colors are used to indicate status:</p> <p>Gray. The Domain Join action has not been attempted. This is the default status that appears when you are using the page to create a new Active Directory configuration.</p> <p>Yellow. Attempting to join the Active Directory domain. This is the default status that appears after saving configuration settings or when any domain join settings are changed in an existing configuration.</p> <p>Green. The attempt was successful. This status indicates that this server can now be used to authenticate users.</p> <p>Red. The attempt to join the Active Directory domain was not successful.</p>

Settings	Guidelines
	<p>Click Update Join to get the latest join status of nodes. If the status appears persistently red, click Reset Join to reinitiate the domain join process. The Reset Join action requires Active Directory administrator credentials.</p> <hr/> <p> For cluster nodes, you might need to click Update Join multiple times to obtain the latest join status of nodes.</p> <hr/> <p>Transient network issues might also cause the join status indicator to appear red. Before reinitiating the join process, ensure that it is not caused by network issues. Make sure your DNS servers can resolve queries to the Active Directory domain controller and that the Active Directory credentials are valid and have the appropriate permissions.</p>
Additional Options	
Authentication Protocol	<p>The system attempts authentication using the protocols you have enabled in the order shown on the configuration page. For example, if you have selected the check boxes for Kerberos and NTLMv2, the system sends the credentials to Kerberos. If Kerberos succeeds, the system does not send the credentials to NTLMv2. If Kerberos is not supported or fails, the system uses NTLMv2 as the next protocol in order.</p> <p>Kerberos. Select this option to enable the Kerberos authentication protocol. Kerberos is the most secure method and is required for Kerberos single sign-on authentication. Kerberos must be enabled if you plan to use Ivanti single sign-on or browser-based agentless single sign-on (SPNEGO).</p> <p>Enable NTLM protocol. Select this option to enable NTLM if you plan to use any of the following features: Machine authentication using Pulse Client, or Windows native 802.1x supplicants. MS-CHAP-based authentication protocols for any 802.1x supplicants. User password management. Role mapping rules based on group membership. If you enable NTLM, select one of the following versions: NTLMv2. This protocol is moderately secure. It is required for machine authentication and MS-CHAP v2 based 802.1x authentication protocols. NTLMv1. This protocol is comparatively less secure. It might be required for compatibility with existing legacy servers, MS-CHAP based servers, and MS-CHAP based 802.1x authentication protocols.</p>

Settings	Guidelines
Trusts	<p>Contact trusted domains. Select this option to contact domain controllers of trusted domains directly without proxying authentication requests and group membership checks through the domain controller.</p> <p>If this option is not selected:</p> <p>Network contact with trusted domains is not permitted, but pass-through authentication using the primary domain is still permitted.</p> <p>Trusted domain user's group lookup for Kerberos SSO and SPNEGO authentication does not work even though user authentication succeeds.</p> <p>Trusted domain user's password-based authentication does not work.</p> <p>Only groups from the domain in which this system is a member are available for use in role mapping when a group search is performed in the server catalog window.</p> <hr/> <p> If you want to restrict trusted domain users and computers (machine authentication) from logging in when this option is not selected, you can define a custom expression based on the ntdomain variable and use it in role mapping rules. For example, if IPS belongs to the domain named Corporate, you can define a custom expression as ntdomain=Corporate and use the custom expression in the role mapping rule of the realm.</p> <hr/>
SPNEGO Single Sign On	Enable SPNEGO . Select this option to support SPNEGO SSO.
	Keytab Upload. Select this option to use the controls to upload the SPNEGO keytab. The keytab must be generated on the Active Directory Service for the SPN. It must match the FQDN used to access this device.
Machine account password change	Enable periodic password change of machine account. Select this option to change the domain machine account password for this configuration.
	Change machine password frequency. Specify a frequency in days. For example, every 30 days.
Logical Auth Server Name	Specify a logical authentication server name.

You can troubleshoot the configurations using the Troubleshooting Tab for the respective server. You will be able to view this option on configuring the respective server. Using the troubleshooting option, you can validate:



- Domain Joint Status
 - Authentication success status
 - DNS Look-up for the respective servers
 - Authentication Statistics
-

Using Kerberos SSO

Kerberos SSO Support Overview

Kerberos single sign-on (SSO) is a method of access control that allows a user to log in once to the client desktop without being prompted again for credentials.

The Kerberos SSO feature uses Kerberos authentication to automatically sign in users with the same credentials they used to access their Windows desktops. After you configure Kerberos SSO, the sign-in dialog box does not appear to users.

Requirements and Limitations

The following requirements and limitations apply to the Kerberos SSO implementation:

- The SSO feature requires a Windows NT Primary Domain Controller (PDC) or Active Directory for user authentication.
- The Kerberos SSO feature is not supported on Windows NT Server 4.0 or earlier
- The clocks on IPS and the Windows Active Directory authentication server must be synchronized to within 2 minutes of each other.
- The Active Directory controller must be deployed in front of IPS.
- The Windows endpoint computers must be joined to the same domain that IPS uses for authentication. Alternatively, make sure the Windows endpoint computers are joined to a domain that has a trust relationship with the domain that IPS uses for authentication.
- Users must sign into their endpoint computers in the domain of the Windows Active Directory authentication server or in a trusted domain.

- The realm Enable SSO option is visible only if the Windows Active Directory authentication server is used for authenticating users of the selected realm.

Enabling Kerberos SSO

To enable Kerberos SSO:

1. Select **Authentication > Auth. Servers**.
2. Select **New Active Directory / Windows NT** and click **New**.
3. Complete the configuration. Enable the Kerberos authentication protocol option.
4. Configure the realm:
 - Select **Administrators > Admin Realms or Users > User Realms**. Specify the realm that must use the Active Directory server to authenticate and authorize administrators and users.
 - Select **Administrators > Admin Realms > Select Realm > Authentication Policy > SSO** to ensure that the Enable SSO option is enabled (the default).

Understanding Multidomain User Authentication

This topic provides an overview of multi domain user authentication with Active Directory and Windows NT.

Multi-Domain User Authentication Overview

The Pulse Secure access management framework allows for multidomain Active Directory and Windows NT authentication. The system authenticates users in the domain that you configure, users in child domains, and users in all domains trusted by the configured domain.

Users in the default domain can sign into the system using just their username, or the default domain and the username in the format default-domain\username.

When you enable trusted domain authentication, users in trusted or child domains can sign in using the name of the trusted or child domain and the username in the format trusted-domain\username. Note that enabling trusted domain authentication adds to the server response time.

Windows NT User Normalization

To support multidomain authentication, the Pulse Secure access management framework uses “normalized” Windows NT credentials when it contacts an Active Directory or Windows NT4 domain controller for authentication. Normalized Windows NT credentials include both the domain name and the username: domain\username. Regardless of how the user signs in (either using just a username or using the domain\username format), the access management framework always processes the username in domain\username format.

When a user signs in using only their username, the access management framework normalizes their Windows NT credentials as default-domain\username. Authentication succeeds only if the user is a member of the default domain.

When a user signs in using the domain\username format, the access management framework attempts to authenticate the user as a member of the domain the user specifies. Authentication succeeds only if the user-specified domain is a trusted or child domain of the default domain. If the user specifies an invalid or untrusted domain, authentication fails.

Two variables, <NTUser> and <NTDomain>, allow you to individually refer to Windows NT domain and username values. The system populates these two variables with the Windows NT domain and username information.

In role mapping rules, when you specify **USER = someusername**, the system treats this rule semantically as **NTUser = someusername AND NTDomain = defaultdomain**.

Kerberos Support

We recommend you configure the Pulse Secure access management framework to use the Kerberos authentication protocol with Windows domain controllers. When a user logs in to the system, the system performs Kerberos authentication and attempts to fetch the Kerberos realm name for the domain controller, as well as all child and trusted realms, using LDAP calls.

You can use Kerberos differently. You can specify the Kerberos realm name when configuring an Active Directory authentication server. We do not recommend this method for two reasons:

You cannot specify more than one realm name. The system cannot then authenticate against child or trusted realms of the realm you specify.

If you misspell the realm name, the system cannot authenticate users against the proper realm.

Windows NT4 Support

The Pulse Secure access management framework does not support Kerberos-based authentication in Windows NT4 domain controllers. The system uses NTLM with a backend Windows NT4 domain controller.

Understanding Active Directory and Windows NT Group Information Support

This topic describes support for polling group information from Active Directory and Windows NT servers.

Active Directory Group Information Overview

The Pulse Secure access management framework supports user group lookup in Domain Local, Domain Global, and Universal groups in the default domain, child domains, and all trusted domains. The system obtains group membership using one of three methods that have different capabilities:

- Group information in User's Security Context—Returns information about the user's Domain Global groups.
- Group information obtained using LDAP search calls—Returns information about the user's Domain Global groups and about the user's Universal groups if the access management framework queries the Global Catalog Server.
- Group information using native RPC calls—Returns information about the user's Domain Local Group.
- With respect to role-mapping rules, the system attempts group lookup in the following order:
 - Checks for all Domain Global groups using the user's security context.
 - Performs an LDAP query to determine the user's group membership.
 - Performs an RPC lookup to determine the user's Domain Local group membership.

Windows NT4 Group Information Overview

The Pulse Secure access management framework supports group lookup in the Domain Local and Domain Global groups created in the default domain, as well as all child and other trusted domains. The system obtains group membership using:

- Domain Global group information from the user's security context.
- Domain Local information using RPC calls.

In the Windows NT4 environment, the system does not use LDAP-based search calls.

Importing and Exporting an Active Directory Mode Configuration

You can use the Maintenance > Import/Export > Import/Export users page to copy an Active Directory mode configuration from one system to another. If Active Directory credentials for joining a domain are not stored in the exported configuration, you must update the configuration to specify them.



Push configuration is not supported for Active Directory mode configurations.

XML Import/Export for the Active Directory mode configuration has limitations. An XML exported Active Directory configuration (standalone/cluster) can be imported to the same system from which it is exported. However, an XML exported Active Directory configuration from a standalone configuration cannot be imported into a cluster configuration. Similarly, an XML exported Active Directory configuration from a cluster cannot be imported into a standalone configuration.

It is not recommended that you import a configuration into a different system than the one from which the configuration was exported. Although the import operation will be successful, the importing system will join the AD domain with the same computer name as the exporting system. When this occurs, the Active Directory disconnects the earlier join from the exporting system.

To work around this, modify the value of the computer-name parameter in the XML file to be unique and then import it to another system. In cluster configurations, in addition to modifying the computer-name parameter, also modify the node parameter for each cluster member to match with the importing cluster node names.

Here are the parameters you must change before importing the XML configuration file of Active Directory:

<nodenames>

```
<node>clusternode1</node>
<computer-name>computer1</computer-name>
</nodenames>
<nodenames>
<node>clusternode2</node>
<computer-name>computer2</computer-name>
</nodenames>
```



You must specify the clear text password within `<password-cleartext>` `</password-cleartext>` tags, in place of `<user-password-encrypted>` `</user-password-encrypted>` tags, before you perform an XML Import of an Active Directory mode configuration.

Using the Anonymous Server

This topic describes integration with the anonymous server.

Anonymous Server Overview

This section describes support for using IPS with the anonymous server.

Understanding the Anonymous Server

The anonymous server is a local authentication server that allows any user to access the system without providing a username and password.

Instead, when a user enters the URL of a sign-in page that is configured to authenticate against an anonymous server, the IPS access management framework bypasses the standard sign-in page and immediately displays the welcome page to the user.

Anonymous Server Feature Support

IPS access management framework supports the following anonymous server features:

- Enables guest access without username or password
- Supports Host Checker scans before allowing a guest device to connect to the network
- Supports firewall enforcement roles and policies to limit the resources available to the guest user

Interoperability Requirements and Limitations

The following limitations apply to the anonymous server configuration and logging:

- You can add only one anonymous server configuration.
- You cannot create an administrator realm that uses the anonymous server. Anonymous administration is not allowed.
- During configuration, you must choose the anonymous server as both the authentication server and the directory or attribute server in the Users > User Realms > General tab.
- For security reasons, you might want to limit the number of users who sign in through an anonymous server at any given time. To do this, use the option on the Users > User Realms > [Realm] > Authentication Policy > Limits tab (where [Realm] is the realm that is configured to use the anonymous server to authenticate users).

Configuring Authentication with the Anonymous Server

To configure authentication with the anonymous server:

1. Select **Authentication > Auth. Servers**.
2. Select **Anonymous Server** and click **New Server** to display the configuration page.
3. Save the configuration.

Monitoring Anonymous User Sessions

The purpose of the anonymous server is to enable unauthenticated access. Therefore, the system does not maintain session tables, and the Anonymous Server configuration page does not have a corresponding Users tab. The system does maintain user access logs for anonymous access. The username is recorded in the user access log as "AnonUser1234". If the user is logging in using the agentless access method, the user access log records the host's IP address. You can view the User Access Log file by navigating to **System > Log/Monitoring**.

The screenshot shows the LogMonitoring interface for User Access. The top navigation bar includes 'Events', 'User Access', 'Admin Access', 'Sensors', 'Client Logs', 'SNMP', 'Statistics', and 'Advanced Settings'. Below this, there are tabs for 'Log', 'Settings', and 'Filters'. The main area displays a search filter 'Standard Standard (default)' and a 'Show 200 items' option. There are buttons for 'Update', 'Reset Query', and 'Save Query'. Below the search area, there are buttons for 'Save Log As...', 'Clear Log', 'Save All Logs', and 'Clear All Logs'. The table below shows log entries with the following data:

Severity	ID	Message
Info	AUT22873	2016-08-31 18:07:53 - e - [10.204.90.240] testUsers@emed, Users] - Logout from 10.204.90.240 (session:5236dc6f)
Info	AUT24414	2016-08-31 18:02:51 - e - [10.204.90.240] testUsers@emed, Users] - Agent login succeeded for testUsers from 10.204.90.240 with Pulse-Secure6.2.5.869 (Windows 7) Pulse5.2.5.869
Info	AUT24326	2016-08-31 18:02:51 - e - [10.204.90.240] testUsers[] - Primary authentication successful for testSystem Local from 10.204.90.240
Info	AUT22873	2016-08-31 17:48:07 - e - [10.204.90.240] testUsers@emed, Users] - Logout from 10.204.90.240 (session:c3a94a6)

Using the Certificate Server

This topic describes integration with the certificate server.

Certificate Server Overview

This section describes support for using IPS with the certificate server.

Understanding the Certificate Server

The certificate server is a local server that allows user authentication based on the digital certificate presented by the user without any other user credentials.

When you use a certificate server, the user experience is similar to anonymous authentication. If the certificate is secured through a hardware or a software token or through a password, the certificate server authentication is very useful. The certificate contains the full distinguished name (DN) and the system extracts the values from the DN and uses it for role mapping rules, authentication policies, and role restrictions.

Feature Support

The Ivanti Policy Secure(IPS) access management framework supports the following certificate server features:

- Certificate directory services to retrieve user attributes in role mapping rules, authentication policies, and role restrictions.
- Load CA-created certificates on the system.
- Load multiple certificates from different CAs for use with different authentication realms.

Interoperability Requirements and Limitations

If you choose a certificate attribute with more than one value, the system uses the first matched value. For example, if you enter <certDN.OU> and the user has two values for the attribute (ou=management, ou=sales), the system uses the "management" value.

To use all values, add the SEP attribute to the variable. For example, if you enter <certDN.OUT SEP=":"> the system uses "management:sales".

Configuring Authentication with the Certificate Server

To configure authentication with the certificate server:

1. Select **Authentication > Auth. Servers**.
2. Select **Certificate Server** and click **New Server** to display the configuration page.
3. Complete the configuration as described in table.
4. Save the configuration.

Auth Servers > New Certificate Server

New Certificate Server

*Name: Label to r

User Name Template: Template

The template can contain textual characters as well as variables for custom expressions and policy conditions. All of the certificate variables are listed below.

Examples:


- <certDN.CN> First CN from the subject DN
- <certAttr.serialNumber> Certificate serial number
- <certAttr.altName.xxx> Where xxx can be:
 - Email The Email alternate name
 - UPN The Principal Name alternate name
 - ... etc
- <certDNText> The complete subject DN
- cert-<certDN.CN> The text "cert-" followed by the first CN from the subject DN

▼ User Record Synchronization

Enable User Record Synchronization

Logical Auth Server Name:

* indicates required field

Settings	Guidelines
Name	Specify a name to identify the server within the system.
User Name Template	<p>Specify a username template. Specify how the system should construct a username. You may use any combination of certificate variables contained in angle brackets and plain text.</p> <hr/> <p> This value populates the <USER> and <USERNAME> session variables for use throughout the rest of the system configuration.</p> <hr/>
Logical Auth Server Name	Specify a logical authentication server name.

Displaying the User Accounts Table

To display user accounts:

1. Select **Authentication > Auth. Servers**.
2. Click the link for the authentication server you want to manage.
3. Click the **Users** tab to display the user accounts table.

The user accounts table includes entries for the accounts that have been created. The Last Sign-in Statistic column shows the last successful sign-in date and time for each user, the user's IP address, and the agent or browser type and version.

4. Use the controls to search for users and manage user accounts:
 - To search for a specific user, enter a username in the Show users named box and click **Update**.



You can use an asterisk (*) as a wildcard, where * represents any number of zero or more characters. For example, to search for all usernames that contain the letters jo, enter *jo*. The search is case-sensitive. To display the entire list of accounts again, type * or delete the field's contents and click **Update**.

-
- To limit the number of users displayed on the page, enter a number in the Show N users box and click **Update**.
 - To terminate the user session and delete the account, select the check box next to the user account record and click **Delete**.

Using an LDAP Server

This topic describes integration with the LDAP server.

LDAP Server Overview

This section describes support for using IPS with the LDAP server.

Understanding LDAP Server

Lightweight Directory Access Protocol (LDAP) facilitates the access of online directory services. The Internet Engineering Task Force (IETF) designed and specified LDAP as a better way to make use of X.500 directories, having found the original Directory Access Protocol (DAP) too complex for average Internet clients to use. LDAP is a relatively simple protocol for updating and searching directories running over TCP/IP.

LDAP directory consists of a collection of attributes with a name, known as a distinguished name (DN). Each of the entry's attributes, known as a relative distinguished name (RDN), has a type and one or more values. The types are typically mnemonic strings, such as CN for common name. The valid values for each field depend on the types.

The full DN is constructed by stringing together RDNs from most specific to least specific, separated by commas, as shown in the following example:

```
cn=Bob_Employee, ou= account_mgr, o=sales, dc=Acme,dc=com.
```

LDAP Feature Support

Pulse Secure access management framework supports the following LDAP features:

- LDAP directory services to retrieve user attributes and group membership in role mapping rules
- Encrypted connections to the LDAP server using LDAP over SSL (LDAPS) or Start Transport Layer Security (TLS)
- Password management feature enabling users who access an LDAP server to manage their passwords using the policies defined on the LDAP server
- Fine-grained password policy (FGP) for Active Directory 2008

Interoperability Requirements and Limitations

The following limitations apply to interoperability with LDAP:

- By default, challenge response protocols are disabled for LDAP servers. Use these protocols only with noninteractive devices (for example, phones), as password management is not possible if these protocols are used for authentication.

- To use the CHAP, EAP-MD5-Challenge, MS-CHAP-V1, and MS-CHAP-V2 protocols, the LDAP server must store the user's password in clear text.
- Backup LDAP servers must be the same version as the primary LDAP server. Also, we recommend that you specify the IP address of a backup LDAP server instead of its hostname, which might accelerate failover processing by eliminating the need to resolve the hostname to an IP address.

Configuring Authentication with an LDAP Server

To configure authentication with an LDAP server:

1. Select **Authentication > Auth. Servers**.
2. Select **LDAP Server** and click **New Server** to display the configuration page.
3. Complete the configuration as described in table.
4. Save the configuration.

Auth Servers > New LDAP Server

New LDAP Server

*Name: Label to reference this server.

*LDAP Server: Name or IP address

*LDAP Port:

Backup LDAP Server1: Name or IP address

Backup LDAP Port1:

Backup LDAP Server2: Name or IP address

Backup LDAP Port2:

LDAP Server Type:

Connection: Unencrypted LDAPS Start TLS

Connection Timeout: Seconds to wait for connection to LDAP server

Search Timeout: Seconds to wait for search results, excluding connection time

Authentication required

In order to use Password Management, you may need to select the 'Authentication required to search LDAP' checkbox below and enter your LDAP administrator DN and password.

Authentication required to search LDAP

Admin DN:

Password:

Backup Admin DN:

Backup Admin Password:

Finding user entries

Specify how to find a user entry

Base DN: example: dc=sales,dc=com

*Filter: example: cn=<USER>

Remove Domain from Windows user names

If users authenticate using Windows user names containing domain prefixes (for example, CORP\joe), it may be necessary to remove the domain prefix in order for authentication to succeed. If you choose this option, the <NTDOMAIN> variable is set to the domain name that was removed from the user name.

Strip domain from Windows user names

Enable Challenge Response open protocols

Because LDAP authentication servers generally do not support these protocols natively and the user's password is encrypted, it is necessary to bind as the administrator to authenticate a user. This prevents the authentication server from performing account and password management, which is used to determine things like disabled accounts or expired passwords. Enable these protocols only if your LDAP store is being used solely for non-interactive devices such as telephones that do not require account or password management functionality.

Enable Challenge-Response open protocols

Determining group membership

If group membership is NOT reflected as attributes of a user's entry, specify how to find a group's entries. Note that these are default settings that you can override on a per-group basis in the Server Catalog.

Base DN: example: dc=sales,dc=com

Filter: example: cn=<GROUPNAME>

Member Attribute: Attribute used to identify members of a static group or groups to which a member belongs



Query Attribute: Attribute used to determine members of a dynamic group


Nested Group Level: Maximum depth of nested group search is [0-10]. 0 to disable the Nested search.

Nested Group Search: Nested groups in Server Catalog Faster, but less flexible
 Search all nested groups Slower, but more flexible

Settings	Guidelines
Name	Specify a name to identify the server within the system.

Settings	Guidelines
Enable Domain Name (enabled)	Select this option to fetch a list of servers from the DNS server.
	Domain Name When you Enable Domain Name, specify the LDAP Domain name that can be mapped to domain controllers by DNS service.
Enable Domain Name (disabled)	Clear this option if you want to manually enter all the domain controllers host names.
	LDAP Server: Specify the LDAP server name or the IP address. Backup LDAP Server1: (Optional) Specify the parameters for backup LDAP server1. The specified backup LDAP server is used for failover processing. The authentication request is first routed to the primary LDAP server, and then to the specified backup servers if the primary server is unreachable.
	Backup LDAP Port1: Specify the parameters for backup LDAP port1.
	Backup LDAP Server2: (Optional) Specify the parameters for backup LDAP server2.
LDAP Port	Specify the LDAP port for the LDAP server. Default port number: 389 (unencrypted connection) Default port number: 636 (SSL connection)
LDAP Server Type	Select the backend LDAP server type from the following choices: Generic Active Directory iPlanet Novell eDirectory Profiler (Policy Secure only)
Connection	Select one of the following options for the connection to the LDAP server: <ul style="list-style-type: none"> • Unencrypted– The device sends the username and password to the LDAP Directory Service in clear text. • LDAPS– The device encrypts the data in the LDAP authentication session using the Secure Socket Layer (SSL) protocol before sending it to the LDAP Directory Service.

Settings	Guidelines
	<ul style="list-style-type: none"> • Start TLS– The device allows both secure and plain requests against an LDAP server on a single connection. <hr/> <ul style="list-style-type: none"> - If you select LDAPS or Start TLS, the Validate Certificate option is displayed for the configured LDAP server(s) and its referral servers. Select this option if the SSL connection uses digital certificate security.  - If you enable validation for the referral servers, make sure your network DNS supports reverse lookup zone. - If you want to verify the server certificates, the root CA and Intermediate CAs must be imported as trusted CAs. <hr/>
Connection Timeout (seconds)	Specify the time to wait for connection to the primary LDAP server, and then to each backup LDAP server. Default: 15 seconds
Search Timeout (seconds)	Specify the time to wait for search results from a connected LDAP server.
Test Connection	<p>(Optional) To verify the connection between Pulse Client and LDAP servers, click the Test Connection button.</p> <hr/> <p> We recommend using the Test Connection function only after saving changes on the LDAP Server Configuration page.</p> <hr/>
Authentication required?	
Authentication required to search LDAP	Select this option to require authentication when performing search or password management operations.

Settings	Guidelines
	<hr/> <ul style="list-style-type: none"> - If you use Active Directory, you must select the Authentication required to search LDAP check box and provide the full DN and password of an account that can reach Active Directory. - You can enable password management on any LDAP server.  - This feature enables users who authenticate through an LDAP server to manage their passwords through the system using the policies defined on the LDAP server. To enable password management on any LDAP server, you must provide primary and backup administrator accounts (with write privileges to the directory) for the administrator DN and backup administrator DN. <hr/>
Admin DN	Specify the administrator DN for queries to the LDAP directory.
Password	Specify the password for the LDAP server.
Backup Admin DN	Specify the backup administrator DN for queries to the LDAP directory, as a fallback when primary Admin DN fails (due to account expiration). The interaction with LDAP directory stops when both primary and backup administrator accounts fail.
Backup Admin Password	Specify the backup administrator password for the LDAP server.
Finding user entries	
Base DN	Specify the base DN under which the users are located. For example, dc=sales,dc=acme, dc=com.
Filter	<p>Specify a unique variable that can be used to do a fine search in the tree. For example, samAccountname= <username> or cn= <username>. Include <username> in the filter to use the username entered on the sign-in page for the search.</p> <p>Specify a filter that returns 0 or 1 user DN's per user; the device uses the first DN returned if more than 1 DN is returned.</p>
Remove Domain from Windows users names?	

Settings	Guidelines
Strip domain from Windows username	Select this option to pass the username without the domain name to the LDAP server.
Enable Challenge-Response open protocols?	
Enable Challenge-Response open protocols	Select this option if you want to use a challenge-response protocol for authentication. By default, these protocols are disabled for LDAP servers because account management is not possible.
Determining group membership	
Base DN	Specify the base DN to search for user groups.
Filter	Specify a unique variable which can be used to do a fine search in the tree. For example, samAccountname= <username> or cn= <GROUPNAME>.
Member Attribute	Specify all the members of a static group. For example, member or uniquemember (iPlanet specific).
Reverse group search	Select this option to start the search from the member instead of the group. This option is available only for Active Directory server types.
Query Attribute	Specify an LDAP query that returns the members of a dynamic group. For example, memberURL.
Nested Group Level	Specify how many levels within a group to search for the user. The higher the number, the longer the query time, so we recommend that you specify to perform the search no more than two levels deep.
Nested Group Search	Select one of the following options: Nested groups in Server Catalog—This option is faster because it can search within the implicit boundaries of the nested group. Search all nested groups—With this option, the device searches the Server Catalog first. If the device finds no match in the catalog, then it queries LDAP to determine if a group member is a subgroup.

Displaying the User Accounts Table

To display user accounts:

1. Select **Authentication > Auth. Servers**.
2. Click the link for the authentication server you want to manage.
3. Click the **Users** tab to display the user accounts table.

The user accounts table includes entries for the accounts that have been created. The Last Sign-in Statistic column shows the last successful sign-in date and time for each user, the user's IP address, and the agent or browser type and version.

4. Use the controls to search for users and manage user accounts:
 - To search for a specific user, enter a username in the Show users named box and click **Update**.



You can use an asterisk (*) as a wildcard, where * represents any number of zero or more characters. For example, to search for all usernames that contain the letters jo, enter *jo*. The search is case-sensitive. To display the entire list of accounts again, type * or delete the field's contents and click **Update**.

-
- To limit the number of users displayed on the page, enter a number in the Show N users box and click **Update**.
 - To terminate the user session and delete the account, select the check box next to the user account record and click **Delete**.

Using the LDAP Password Management Feature

This topic describes support and limitations for LDAP password management.

LDAP Password Management Feature Overview

The password management feature enables users who access an LDAP server to manage their passwords through the Pulse Secure access management framework using the policies defined on the LDAP server. For example, if a user tries to sign in to the system with an LDAP password that is about to expire, the system notices the user through the interface, and then passes the user's response back to the LDAP server without requiring the user to sign in to the LDAP server separately.

Users, administrators, and help desk administrators who work in environments where passwords have set expiration times may find the password management feature very helpful. If users are not informed that their passwords are about to expire, they can change them themselves through the system rather than call the help desk.

Once this feature is enabled, the system performs a series of queries to determine user account information, such as when the user's password was last set, whether the account is expired, and so on. The Pulse Secure access management framework does this by using its internal LDAP or Samba client. Many servers, such as Microsoft Active Directory or Sun iPlanet, offer an Administrative Console to configure account and password options.

LDAP-based password management works with only three types of LDAP servers:

- Microsoft Active Directory. For Active Directory, password policy attributes can be configured in the user entry container level or any organization level above the user container. If these attributes are configured at multiple levels, the level closest to the user node takes precedence. The password management feature is not supported on the Active Directory Global Catalog because password policy attributes are not fully populated in the Active Directory Global Catalog.
- For Active Directory 2008, the Pulse Secure access management framework supports the Fine Grained Password Policy (FGP) configured in the AD user container.
- Sun Microsystems iPlanet
- Novell eDirectory

LDAP-based password management does not work on generic LDAP servers such as OpenLDAP.

The system relies on the back-end server to pinpoint the cause of error when a password change operation fails. However, although LDAP servers may report errors accurately to human operators, they do not always do so when communicating programmatically to systems. Therefore, reported errors might be generic or cryptic.

The system does not support customized password policies.

Enabling LDAP Password Management

To enable password management, you must first create an instance of the LDAP server. Next, you associate the LDAP server with the applicable realms. Finally, you select the enable password management feature at the realm level.

LDAP Password Management Support

The Pulse Secure access management framework supports password management with the following LDAP directories:

- Microsoft Active Directory/Windows NT
- Sun iPlanet
- Novell eDirectory
- Generic LDAP directories, such as IBM Secure Directory and OpenLDAP

The below table describes supported password management functions, their corresponding function names in the individual LDAP directories, and any additional relevant details. These functions must be set through the LDAP server itself before the system can pass the corresponding messages, functions, and restrictions to end users.

The Active Directory attribute names shown are specific to the Domain Security Policy object. Similar attributes for the corresponding functions are used for the Active Directory 2008 Fine-Grained Password Policy. Refer to Microsoft documentation for details.

When authenticating against a generic LDAP server, such as IBM Secure Directory, the system supports only authentication and allowing users to change their passwords. Password management functions are not supported when the CHAP family protocols are used for authentication. All functions are available when the JUAC protocol is used for authentication.

Function	Active Directory	iPlanet	eDirectory	Generic
Authenticate user	unicodePwd	userPassword	userPassword	userPassword
Allow user to change password if enabled	Server tells us in bind response (uses ntSecurityDescriptor)	If passwordChange == ON	If passwordAllowChange == TRUE	Yes
Log out user after password change	Yes	Yes	Yes	Yes

Function	Active Directory	iPlanet	eDirectory	Generic
Force password change at next log in	If pwdLastSet == 0	If passwordMustChange == ON	If pwdMustChange == TRUE	-
Expired password notification	userAccountControl == 0x80000	If Bind Response includes OID 2.16.840.1.113730.3.4.4 == 0	Check date/time value	-
Password expiration notification (in X days/hours)	if pwdLastSet - now() < maxPwdAge - 14 days (Read from domain attributes) (The system displays warning if less than 14 days)	If Bind Response includes control OID 2.16.840.1.113730.3.4.5 (contains date/time) (The system displays warning if less than 14 days)	If now() - passwordExpirationTime < 14 days (The system displays warning if less than 14 days)	-
Disallow authentication if "account disabled/locked"	userAccountControl == 0x2 (Disabled) accountExpires userAccountControl == 0x10 (Locked) lockoutTime	Bind ErrorCode: 53 "Account Inactivated" Bind Error Code: 19 "Exceed Password Retry Limit"	Bind ErrorCode: 53 "Account Expired" Bind ErrorCode: 53 "Login Lockout"	-
Honor "password history"	Server tells us in bind response	Server tells us in bind response	Server tells us in bind response	-
Enforce "minimum password length"	If set, the system displays message telling user minPwdLength	If set, the system displays message telling user passwordMinLength	If set, the system displays message telling user passwordMinimumLength	-

Function	Active Directory	iPlanet	eDirectory	Generic
Disallow user from changing password too soon	If pwdLastSet - now() < minPwdAge, then we disallow	If passwordMinAge > 0, then if now() is earlier than passwordAllowChangeTime, then we disallow	Server tells us in bind response	-
Honor "password complexity"	If pwdProperties == 0x1, then enabled. Complexity means the new password does not contain username, first or last name, and must contain characters from 3 of the following 4 categories: English uppercase, English lowercase, Digits, and Non-alphabetic characters (ex. !, \$, %)	Server tells us in bind response	Server tells us in bind response	-

Note the following expected behavior:

- When you select the User must change password after reset option on the iPlanet server, you must also reset the user password before this function takes effect. This issue is a limitation of iPlanet.

- The system displays a warning about password expiration only if the password is scheduled to expire in 14 days or less. The system displays the message during each sign-in attempt. The warning message contains the remaining number of days, hours, and minutes that the user has to change the password before it expires on the server. The default value is 14 days, but you can change it on the password configuration page of the admin console.

LDAP Password Management for Windows AD Versions

The Pulse Secure access management framework supports password management with the following Windows servers:

- Microsoft Active Directory 2008
- Microsoft Active Directory 2003
- Windows NT 4.0

Table describes supported password management functions. These functions are not supported for a layer 2 connection when CHAP, MS-CHAP, or PAP are used as authentication protocols.

Function	Active Directory	Active Directory 2003	Active Directory 2008 FGP	Windows NT
Authenticate user	Yes	Yes	Yes	Yes
Allow user to change password if licensed and if enabled	Yes	Yes	Yes	Yes
Log out user after password change	Yes	Yes	Yes	Yes
Force password change at next log in	Yes	Yes	Yes	Yes
Password expired notification	Yes	Yes	Yes	Yes
Account disabled	Yes	Yes	Yes	Yes
Account expired	Yes	Yes	Yes	Yes

Note the following expected behavior:

- Changes on the Active Directory domain security policy can take 5 minutes or longer to propagate among Active Directory domain controllers. Additionally, this information does not propagate to the domain controller on which it was originally configured for the same time period. This issue is a limitation of Active Directory.
- When changing passwords in Active Directory using LDAP, the system automatically switches to LDAPS, even if LDAPS is not the configured LDAP method. To support LDAPS on the Active Directory server, you must install a valid SSL certificate into the server's personal certificate store. The certificate must be signed by a trusted CA, and the CN in the certificate's Subject field must contain the exact hostname of the Active Directory server, (for example: adsrv1.company.com). To install the certificate, select the Certificates Snap-In in the Microsoft Management Console (MMC).
- The Account Expires option in the User Account Properties tab only changes when the account expires, not when the password expires. Microsoft Active Directory calculates the password expiration using the Maximum Password Age and Password Last Set values retrieved from the User object and Fine-Grained Password Policy objects or the Domain Security Policy LDAP objects.
- The system displays a warning about password expiration only if the password is scheduled to expire in 14 days or less. The system displays the message during each sign-in attempt. The warning message contains the remaining number of days, hours, and minutes that the user has to change the password before it expires on the server. The default value is 14 days, but you can change it on the password configuration page of the admin console.

Troubleshooting LDAP Password Management

When you troubleshoot, provide any pertinent system logs, server logs, configuration information, and a TCP trace from the system. If you are using LDAPS, switch to the "Unencrypted" LDAP option LDAP server configuration while taking the LDAP TCP traces.

Using the MAC Address Authentication Server

This topic describes how to use the MAC address authentication server.

MAC Address Authentication Server Overview

This section describes IPS MAC address authentication solution.

Understanding MAC Address Authentication

MAC address authentication is port-based security typically deployed at the edge of the network to enable secure access for non-user devices, such as IP phones, printers, and network attached storage devices. The Ivanti MAC address authentication solution uses IPS 802.1x framework. When a device connects to a switch, the switch forwards the MAC address as the log in credential to IPS RADIUS server. With MAC-based authentication, the MAC address serves as both the username and the password. The RADIUS server consults the authentication server and sends back a RADIUS return attribute based on authentication results.

BEST PRACTICE: MAC-based authentication is not as secure as agent access or agentless access authentication. MAC addresses are not generally guarded as secrets, so an attacker can spoof a MAC address and impersonate a device to gain network access. To reduce risk of an exploit, create a special VLAN for each device type.

MAC Address Authentication Server Feature Support

The MAC address authentication server is a local authentication server that supports both a local database of records and integration with LDAP servers. You can add entries manually or by reference to LDAP servers. The address table for each local MAC address authentication server is limited to 500 entries. We recommend you use LDAP for large-scale projects.

Interoperability Requirements and Limitations

Integration with an LDAP server requires the LDAP server to communicate with IPS internal interface.

MAC Address Authentication Framework Configuration Overview

The MAC address authentication framework is similar to the user access management framework. It involves configuration of a MAC address authentication server, MAC address realm, and roles.

To implement the MAC address authentication framework:

1. If necessary, use the Authentication Protocols Sets page to add the protocols that your Ethernet switches use for MAC authentication to IPS 802.1x protocol set. Select Authentication > Signing In > Authentication Protocols Sets.

The HP and Cisco switches can use CHAP and EAP-MD5-Challenge protocols for MAC address authentication with the username (the MAC address) as the clear text password. By default, the Nortel switch uses PAP, with a password in the format .<MAC Address>. We recommend using PAP with the Nortel switch.

2. Create LDAP server configurations for the external LDAP servers used to maintain MAC address records.
3. Create a MAC address authentication server.
4. Create Users.



Radius Return Attributes from the dictionaries is pre-populated to the Server Catalog of MAC Auth server so that they are available under the custom attributes for a specific user.

5. Create roles for agentless access.
6. Create a MAC address authentication realm that uses the MAC address authentication server and role mapping rules that sort MAC address authentication requests into roles according to your security policy design.

802.1x Framework Configuration Overview

The MAC address authentication solution uses Ivanti Policy Secure 802.1x framework.

To implement the 802.1x framework:

- Complete the Location Group configuration.
- Complete the RADIUS Client configuration.
- Complete the RADIUS Return Attributes Policy configuration.

Ethernet Switch MAC Address Authentication Configuration Overview

The MAC address solution depends on the Ethernet switch configuration.

To configure MAC address authentication on the Ethernet switch:

- Configure the switch as an 802.1x authenticator and enable MAC RADIUS protocols.
- Configure RADIUS client communication with IPS RADIUS server.
- Configure Ethernet switching options and VLANs to provision VLANs for non-user devices.

Configuring the EX Series Switch

The nonsupplicant devices, such as VoIP phones, connect to the network through an EX Series switch using MAC RADIUS authentication. You configure the following EX Series features to support this solution:

- Configure the switch as an 802.1x authenticator and enable MAC RADIUS protocols.
- Configure RADIUS client communication with IPS RADIUS server.
- Configure Ethernet switching options and VLANs to provision a VLAN for VoIP phones.

The following example shows commands that configure the ge-0/1/0.0 and ge-0/1/1.0 interfaces as 802.1x authenticators, enable MAC RADIUS protocols, and create a reference to the authentication profile used for integration with IPS RADIUS server:

```
set protocols dot1x authenticator authentication-profile-name pulsesecure-access-
profile
set protocols dot1x authenticator interface ge-0/1/0.0 supplicant multiple
set protocols dot1x authenticator interface ge-0/1/0.0 transmit-period 15
set protocols dot1x authenticator interface ge-0/1/0.0 mac-radius
set protocols dot1x authenticator interface ge-0/1/0.0 maximum-requests 2
set protocols dot1x authenticator interface ge-0/1/0.0 server-fail vlan-name
enterprise
set protocols dot1x authenticator interface ge-0/1/1.0 supplicant multiple
set protocols dot1x authenticator interface ge-0/1/1.0 quiet-period 5
set protocols dot1x authenticator interface ge-0/1/1.0 transmit-period 15
set protocols dot1x authenticator interface ge-0/1/1.0 mac-radius
set protocols dot1x authenticator interface ge-0/1/1.0 supplicant-timeout 15
set protocols dot1x authenticator interface ge-0/1/1.0 maximum-requests 2
set protocols dot1x authenticator interface ge-0/1/1.0 guest-vlan guest
set protocols dot1x authenticator interface ge-0/1/1.0 server-reject-vlan vlan-name
guest
```



```
set protocols dot1x authenticator interface ge-0/1/1.0 server-fail vlan-name
enterprise
```

The following example shows commands that configure the access profile for IPS RADIUS server and the RADIUS client connection to it:

```
set access radius-server 10.0.1.5 port 1812
set access radius-server 10.0.1.5 secret "$9$JLZHmzF/t0I69Icrv7N24aZikmfT3/C"
set access radius-server 10.0.1.5 timeout 5
set access radius-server 10.0.1.5 retry 3
set access profile pulsesecure-access-profile authentication-order radius
set access profile pulsesecure-access-profile radius authentication-server 10.0.1.5
set access profile pulsesecure-access-profile radius accounting-server 10.0.1.5
set access profile pulsesecure-access-profile accounting order radius
```

The following example shows commands that configure the Ethernet switching options and VLAN used for VoIP phones:

```
set ethernet-switching-options voip interface ge-0/0/10.0 vlan VoIP_Phone
set ethernet-switching-options voip interface ge-0/0/11.0 vlan VoIP_Phone
set ethernet-switching-options voip interface ge-0/0/8.0 vlan VoIP_Phone
set ethernet-switching-options voip interface ge-0/0/9.0 vlan VoIP_Phone
set ethernet-switching-options voip interface ge-0/0/6.0 vlan VoIP_Phone
set ethernet-switching-options voip interface ge-0/0/7.0 vlan VoIP_Phone
set ethernet-switching-options voip interface ge-0/0/4.0 vlan VoIP_Phone
set ethernet-switching-options voip interface ge-0/0/5.0 vlan VoIP_Phone
set ethernet-switching-options voip interface ge-0/1/0.0 vlan VoIP_Phone
set ethernet-switching-options voip interface ge-0/1/1.0 vlan VoIP_Phone
set vlans VoIP_Phone description "VoIP Phones"
set vlans VoIP_Phone vlan-id 5
```

The following example shows the complete configuration hierarchy for the Ethernet switch configuration:

```
system {
  host-name Demo_EX;
  root-authentication {
    encrypted-password "$1$0OuTchlK$/Z6JTJ/I9BnjTsKAoefLS."; ## SECRET-DATA
  }
  log in {
    user admin {
      full-name Administrator;
      uid 2000;
      class super-user;
      authentication {
```

```
encrypted-password "$1$RKLp.iDP$m//eueOcF.rExsnQXuZNb/"; ## SECRET-DATA
}
}
}
services {
ssh;
telnet;
web-management {
http;
}
}
syslog {
user * {
any emergency;
}
file messages {
any notice;
authorization info;
}
}
}
chassis {
alarm {
management-ethernet {
link-down ignore;
}
}
}
interfaces {
ge-0/0/0 {
unit 0 {
family ethernet-switching {
port-mode trunk;
vlan {
members [ enterprise guest remediation VoIP_Phone ];
}
native-vlan-id default;
}
}
}
ge-0/0/1 {
```

```
unit 0 {
family ethernet-switching {
port-mode trunk;
vlan {
members [ enterprise guest remediation VoIP_Phone ];
}
native-vlan-id default;
}
}
}
ge-0/0/2 {
unit 0 {
family ethernet-switching {
port-mode trunk;
vlan {
members [ enterprise guest remediation VoIP_Phone ];
}
native-vlan-id default;
}
}
}
ge-0/0/3 {
unit 0 {
family ethernet-switching {
port-mode trunk;
vlan {
members [ enterprise guest remediation VoIP_Phone ];
}
native-vlan-id default;
}
}
}
ge-0/0/4 {
unit 0 {
family ethernet-switching {
port-mode access;
}
}
}
ge-0/0/5 {
unit 0 {
```

```
family ethernet-switching {
port-mode access;
}
}
}
ge-0/0/6 {
unit 0 {
family ethernet-switching {
port-mode access;
}
}
}
ge-0/0/7 {
unit 0 {
family ethernet-switching {
port-mode access;
}
}
}
ge-0/0/8 {
unit 0 {
family ethernet-switching {
port-mode access;
}
}
}
ge-0/0/9 {
unit 0 {
family ethernet-switching {
port-mode access;
}
}
}
ge-0/0/10 {
unit 0 {
family ethernet-switching {
port-mode access;
}
}
}
ge-0/0/11 {
```

```
unit 0 {
  family ethernet-switching {
    port-mode access;
  }
}

ge-0/1/0 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
    }
  }
}

ge-0/1/1 {
  unit 0 {
    family ethernet-switching {
      port-mode access;
    }
  }
}

vlan {
  unit 0 {
    family inet {
      address 10.0.1.10/24;
    }
  }
}

routing-options {
  static {
    route 0.0.0.0/0 next-hop 10.0.1.1;
  }
}

protocols {
  dot1x {
    authenticator {
      authentication-profile-name pulsesecure-access-profile;
    }
    interface {
      ge-0/1/0.0 {
        supplicant multiple;
        transmit-period 15;
      }
    }
  }
}
```

```
mac-radius;
maximum-requests 2;
server-fail vlan-name enterprise;
}
ge-0/1/1.0 {
supplicant multiple;
quiet-period 5;
transmit-period 15;
mac-radius;
supplicant-timeout 15;
maximum-requests 2;
guest-vlan guest;
server-reject-vlan guest;
server-fail vlan-name enterprise;
}
}
}
}
}
access {
radius-server {
10.0.1.5 {
port 1812;
secret "$9$JLZHmzF/t0I69Icrv7N24aZikmft3/C"; ## SECRET-DATA
timeout 5;
retry 3;
}
}
profile pulsesecure-access-profile {
authentication-order radius;
radius {
authentication-server 10.0.1.5;
accounting-server 10.0.1.5;
}
accounting {
order radius;
}
}
}
ethernet-switching-options {
voip {
```

```
interface ge-0/0/10.0 {
vlan VoIP_Phone;
}
interface ge-0/0/11.0 {
vlan VoIP_Phone;
}
interface ge-0/0/8.0 {
vlan VoIP_Phone;
}
interface ge-0/0/9.0 {
vlan VoIP_Phone;
}
interface ge-0/0/6.0 {
vlan VoIP_Phone;
}
interface ge-0/0/7.0 {
vlan VoIP_Phone;
}
interface ge-0/0/4.0 {
vlan VoIP_Phone;
}
interface ge-0/0/5.0 {
vlan VoIP_Phone;
}
interface ge-0/1/0.0 {
vlan VoIP_Phone;
}
interface ge-0/1/1.0 {
vlan VoIP_Phone;
}
}
}
}
vlans {
VoIP_Phone {
vlan-id 5;
}
default {
vlan-id 1;
interface {
ge-0/0/4.0;
ge-0/0/5.0;
```

```
    }
    13-interface vlan.0;
  }
  enterprise {
    vlan-id 2;
    interface {
      inactive: ge-0/0/5.0;
      ge-0/0/6.0;
      ge-0/0/7.0;
      ge-0/1/0.0;
      ge-0/1/1.0;
    }
  }
  guest {
    vlan-id 3;
    interface {
      ge-0/0/8.0;
      ge-0/0/9.0;
    }
  }
  remediation {
    vlan-id 4;
    interface {
      ge-0/0/10.0;
      ge-0/0/11.0;
    }
  }
  }
  poe {
    interface all;
  }
}
```

In addition to the configuration for the MAC authentication solution shown above, you can also configure the switch to send data (SNMP traps) to the Beacon Endpoint Profiler for use in profiling. The following example commands configure SNMP traps to the Beacon Endpoint Profiler. The Beacon Endpoint Profiler can use the traps to build profile entries:

```
set snmp description EX4200-VOIP-Switch
set snmp contact ex-admin@company.com
set snmp view jweb-view-all oid .1 include
set snmp community public view jweb-view-all
```



```
set snmp community public authorization read-only
set snmp community public clients <BeaconEndpointProfilerIPAddressOrSubnet>
set snmp trap-group Beacon version v2
set snmp trap-group Beacon categories link
set snmp trap-group Beacon targets <BeaconEndpointProfilerIPAddress>
```



To verify that the Beacon Endpoint Profiler can read the EX Series MIB, run the following command from the Beacon Endpoint Profiler command line:

```
snmpwalk -v 2c -c public <EXseriesIPAddress>
```

Using an NIS Server

This topic describes integration with the NIS server.

NIS Server Overview

This section describes support for using IPS with the NIS server.

Understanding NIS Server

Network Information Service (NIS) is an authentication server that allows a central server to manage password authentication, hosts, services, and so on.

When you use an NIS server as the authentication and authorization service for your Pulse Secure access management framework, users can sign in to IPS using the same username and password that is used for the NIS server.

Feature Support

Pulse Secure access management framework supports the following NIS server features:

- Password management feature enables users who access an NIS server to manage their policies defined on the NIS server.
- Integrates NIS map data for passwords, groups, and hosts with corresponding objects in Active Directory.
- Allows migration of NIS domains to Active Directory.

Interoperability Requirements and Limitations

The following limitations apply when defining and monitoring an NIS server instance:

- You can only use NIS authentication with the system if your passwords are stored on the NIS server using Crypt or MD5 formats.
- You can only add one NIS server configuration to the system, but you can use that configuration to authenticate any number of realms.
- The username submitted to the system cannot contain two consecutive tilde symbols (~~).

Configuring Authentication with an NIS Server

To configure authentication with the NIS server:

1. Select **Authentication > Auth.Servers**.
2. Select **NIS Server** and click **New Server** to display the configuration page.
3. Complete the configuration as described in table.
4. Save the configuration.

Settings	Guidelines
Name	Specify a name to identify the server within the system.
NIS Server	Specify the name or IP address of the NIS server.
NIS Domain	Specify the domain name for the NIS server.

Using a RADIUS Server

This topic describes integration with the RADIUS server.

RADIUS Server Overview

This section describes support for using an external RADIUS server.

Understanding RADIUS Server

A Remote Authentication Dial-In User Service (RADIUS) server is a type of server that allows you to centralize authentication and accounting for users.

The following authentication schemes are supported:

- Access-Request—The user enters the username and password to request access to RADIUS server.
- Access-Accept—The user is authenticated.
- Access-Reject—The user is not authenticated and is prompted to reenter the username and password, or access is denied.
- Access-Challenge—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.

Feature Support

Pulse Secure access management framework supports the following RADIUS features:

- RADIUS authentication.
- RADIUS attributes that can be used in role mapping.
- RADIUS directory services to retrieve user attributes in role-mapping rules.
- RADIUS accounting to track the services and the network resources used.
- RADIUS proxy to configure your external RADIUS server as an inner or outer proxy target. When you specify RADIUS proxy, some fields in the RADIUS server configuration page are not

applicable. This feature is supported only on IPS.

- RADIUS Disconnect messages.

Using Challenge Expressions

The Pulse Secure access management framework supports the RSA Authentication Manager using the RADIUS protocol and a SecurID token (available from Security Dynamics). If you use SecurID to authenticate users, they must supply a user ID and the concatenation of a PIN and a token value.

When you define a RADIUS server, the Pulse Secure access management framework allows administrators to use hard-coded (default) challenge expressions that support Defender 4.0 and some RADIUS server implementations (such as Steel-Belted RADIUS and RSA RADIUS) or to enter custom challenge expressions that allow the system to work with many different RADIUS implementations and new versions of the RADIUS server, such as Defender 5.0. The system looks for the response in the Access-Challenge packet from the server and issues an appropriate Next Token, New PIN, or Generic Passcode challenge to the user.

Using CASQUE Authentication

CASQUE authentication uses a token-based challenge/response authentication mechanism employing a CASQUE player installed on the client system. Once configured with CASQUE authentication, the RADIUS server issues a challenge with a response matching the custom challenge expression (:([0-9a-zA-Z/+ =] +):). The system then generates an intermediate page that automatically launches the CASQUE player installed on the user's system.

PassGo Defender

If you are using a PassGo Defender RADIUS server, the user sign-in process is as follows:

1. The user is prompted for and enters a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The RADIUS server sends a unique challenge string to the system. The system displays this challenge string to the user.
4. The user enters the challenge string in a Defender token and the token generates a response string.
5. The user enters the response string on the system and clicks **Sign In**.

Using RADIUS Attributes

Table describes the RADIUS attributes that are supported in RADIUS role-mapping.

Attribute	Description
ARAP-Challenge-Response	Contains the response to the challenge of a dial-in client. Sent in an Access-Accept packet with Framed-Protocol of ARAP.
ARAP-Features	Includes password information that the network access server (NAS) must send to the user in an ARAP feature flags packet. Sent in an Access-Accept packet with Framed- Protocol of ARAP.
ARAP-Password	Appears in an Access-Request packet containing a Framed-Protocol of ARAP. Only one of User-Password, CHAP-Password, or ARAP-Password must be included in an Access-Request, or one or more EAP-Messages.
ARAP-Security	Identifies the ARAP security module to be used in an Access-Challenge packet.
ARAP-Security-Data	Contains the actual security module challenge or response, and is in Access-Challenge and Access-Request packets.
ARAP-Zone-Access	Indicates how to use the ARAP zone list for the user.
Access-Accept	Provides specific configuration information necessary to begin delivery of service to the user.
Access-Challenge	Sends the user a challenge requiring a response, and the RADIUS server must respond to the Access-Request by transmitting a packet with the Code field set to 11 (Access-Challenge).
Access-Reject	Transmits a packet with the Code field set to 3 (Access-Reject) if any value of the received Attributes is not acceptable.
Access-Request	Conveys information specifying user access to a specific NAS, and any special services requested for that user.
Accounting-Request	Conveys information used to provide accounting for a service provided to a user.
Accounting-Response	Acknowledges that the Accounting-Request has been received and recorded successfully.

Attribute	Description
Acct-Authentic	Indicates how the user was authenticated, whether by RADIUS, the NAS itself, or another remote authentication protocol.
Acct-Delay-Time	Indicates how many seconds the client has been trying to send this record.
Acct-Input-Gigawords	Indicates how many times the Acct-Input-Octets counter has wrapped around 2^{32} over the course of this service being provided.
Acct-Input-Octets	Indicates how many octets have been received from the port during the current session.
Acct-Input-Packets	Indicates how many packets have been received from the port during the session provided to a Framed User.
Acct-Interim-Interval	Indicates the number of seconds between each interim update in seconds for this specific session.
Acct-Link-Count	Indicates the count of links known to have been in each multilink session at the time the accounting record is generated.
Acct-Multi-Session-Id	Indicates a unique Accounting ID to make it easy to link together multiple related sessions in a log file.
Acct-Output-Gigawords	Indicates how many times the Acct-Output-Octets counter has wrapped around 2^{32} during the current session.
Acct-Output-Octets	Indicates how many octets have been sent to the port during this session.
Acct-Output-Packets	Indicates how many packets have been sent to the port during this session to a Framed User.
Acct-Session-Id	Indicates a unique Accounting ID to make it easy to match start and stop records in a log file.
Acct-Session-Time	Indicates how many seconds the user has received service.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop).
Acct-Terminate-Cause	Indicates how the session was terminated.

Attribute	Description
Acct-Tunnel-Connection	Indicates the identifier assigned to the tunnel session.
Acct-Tunnel-Packets-Lost	Indicates the number of packets lost on a given link.
CHAP-Challenge	Contains the Challenge Handshake Authentication Protocol (CHAP) challenge sent by the NAS to a PPP CHAP user.
CHAP-Password	Indicates the response value provided by a PPP CHAP user in response to the challenge.
Callback-Id	Indicates the name of a location to be called, to be interpreted by the NAS.
Callback-Number	The dialing string to be used for callback.
Called-Station-Id	Allows the NAS to send the phone number that the user called, using Dialed Number Identification Service (DNIS) or similar technology.
Calling-Station-Id	Allows the NAS to send the phone number that the call came from, using Automatic Number Identification (ANI) or similar technology.
Class	Sent by the server to the client in an Access-Accept and then sent unmodified by the client to the accounting server as part of the Accounting-Request packet, if accounting is supported.
Configuration-Token	Used in large distributed authentication networks based on proxy.
Connect-Info	Sent from the NAS to indicate the nature of the user's connection.
EAP-Message	Encapsulates Extended Access Protocol [3] packets to allow the NAS to authenticate dial-in users by means of EAP without having to understand the EAP protocol.
Event-Timestamp	Records the time that this event occurred on the NAS, in seconds since January 1, 1970 00:00 UTC.
Egress -VLAN-ID	The Egress-VLANID attribute represents an allowed Egress VLANID for this port, indicating if the VLANID is allowed for tagged or untagged frames as well as the VLANID.

Attribute	Description
Egress-VLAN-Name	The Egress-VLAN-Name attribute represents an allowed VLAN for this port. It is similar to the Egress-VLANID attribute, except that the VLAN-ID itself is not specified or known; rather, the VLAN name is used to identify the VLAN within the system.
Filter-Id	Indicates the name of the filter list for this user.
Framed-AppleTalk-Link	Indicates the AppleTalk network number used for the serial link to the user, which is another AppleTalk router.
Framed-AppleTalk-Network	Indicates the AppleTalk Network number which the NAS can probe to allocate an AppleTalk node for the user.
Framed-AppleTalk-Zone	Indicates the AppleTalk Default Zone to be used for this user.
Framed-Compression	Indicates the compression protocol to be used for the link.
Framed-IP-Address	Indicates the address to be configured for the user.
Framed-IP-Netmask	Indicates the IP netmask to be configured for the user when the user is a router to a network.
Framed-IPv6-Pool	Contains the name of an assigned pool used to assign an IPv6 prefix for the user.
Framed-IPv6-Prefix	Indicates an IPv6 prefix (and corresponding route) to be configured for the user.
Framed-IPv6-Route	Indicates the routing information to be configured for the user on the NAS.
Framed-IPv6-Address	Indicates an IPv6 address assigned to NAS interface of the host.
Framed-Interface-Id	Indicates the IPv6 interface identifier to be configured for the user.
Framed-IPX-Network	Indicates the IPX Network number to be configured for the user.

Attribute	Description
Framed-MTU	Indicates the maximum transmission unit to be configured for the user, when it is not negotiated by some other means (such as PPP).
Framed-Pool	Indicates the name of an assigned address pool used to assign an address for the user.
Framed-Protocol	Indicates the framing to be used for framed access.
Framed-Route	Indicates the routing information to be configured for the user on the NAS.
Framed-Routing	Indicates the routing method for the user, when the user is a router to a network.
Idle-Timeout	Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.
Ingress-Filters	<p>The Ingress-Filters attribute corresponds to the Ingress Filter per-port variable. Supports the following values:</p> <p>Disabled=2 Enabled= 1</p> <p>When the attribute has the value "Enabled", the set of VLANs that are allowed to ingress a port must match the set of VLANs that are allowed to egress a port.</p>
Keep-Alives	Uses SNMP instead of keepalives.
Login-IP-Host	Indicates the system with which to connect the user when the Login-Service Attribute is included.
Login-IPv6-Host	Indicates the system with which to connect the user when the Login-Service Attribute is included.
Login-LAT-Group	Contains a string identifying the LAT group codes that this user is authorized to use.
Login-LAT-Node	Indicates the node with which the user is to be automatically connected by LAT.
Login-LAT-Port	Indicates the port with which the user is to be connected by LAT.
Login-LAT-Service	Indicates the system with which the user is to be connected by LAT.

Attribute	Description
Login-Service	Indicates the service to use to connect the user to the log in host.
Login-TCP-Port	Indicates the TCP port with which the user is to be connected when the Login-Service Attribute is also present.
MS-ARAP-Challenge	Only present in an Access-Request packet containing a Framed-Protocol Attribute with the value 3 (ARAP).
MS-ARAP-Password-Change-Reason	Indicates the reason for a server-initiated password change.
MS-Acct-Auth-Type	Represents the method used to authenticate the dial-up user.
MS-Acct-EAP-Type	Represents the Extensible Authentication Protocol (EAP) type used to authenticate the dial-up user.
MS-BAP-Usage	Describes whether the use of BAP is allowed, disallowed, or required on new multilink calls.
MS-CHAP-CPW-1	Allows the user to change password if it has expired.
MS-CHAP-CPW-2	Allows the user to change password if it has expired.
MS-CHAP-Challenge	Contains the challenge sent by a NAS to a MS-CHAP user.
MS-CHAP-Domain	Indicates the Windows NT domain in which the user was authenticated.
MS-CHAP-Error	Contains error data related to the preceding MS-CHAP exchange.
MS-CHAP-LM-Enc-PW	Contains the new Windows NT password encrypted with the old LAN Manager password hash.
MS-CHAP-MPPE-Keys	Contains two session keys for use by the Microsoft Point-to-Point Encryption (MPPE).
MS-CHAP-NT-Enc-PW	Contains the new Windows NT password encrypted with the old Windows NT password hash.
MS-CHAP-Response	Contains the response value provided by a PPP MS-CHAP user in response to the challenge.

Attribute	Description
MS-CHAP2-CPW	Allows the user to change password if it has expired.
MS-CHAP2-Response	Contains the response value provided by an MS- CHAP-V2 peer in response to the challenge.
MS-CHAP2-Success	Contains a 42-octet authenticator response string.
MS-Filter	Transmits traffic filters.
MS-Link-Drop-Time-Limit	Indicates the length of time (in seconds) that a link must be underutilized before it is dropped.
MS-Link-Utilization-Threshold	Represents the percentage of available bandwidth utilization below which the link must fall before the link is eligible for termination.
MS-MPPE-Encryption-Policy	Signifies whether the use of encryption is allowed or required.
MS-MPPE-Encryption-Types	Signifies the types of encryption available for use with MPPE.
MS-MPPE-Recv-Key	Contains a session key for use by the MPPE.
MS-MPPE-Send-Key	Contains a session key for use by the MPPE.
MS-New-ARAP-Password	Transmits the new ARAP password during an ARAP password change operation.
MS-Old-ARAP-Password	Transmits the old ARAP password during an ARAP password change operation.
MS-Primary-DNS-Server	Indicates the address of the primary domain name server (DNS) server to be used by the PPP peer.
MS-Primary-NBNS-Server	Indicates the address of the primary NetBIOS name server (NBNS) server to be used by the PPP peer.
MS-RAS-Vendor	Indicates the manufacturer of the RADIUS client machine.
MS-RAS-Version	Indicates the version of the RADIUS client software.

Attribute	Description
MS-Secondary-DNS-Server	Indicates the address of the secondary DNS server to be used by the PPP peer.
MS-Secondary-NBNS-Server	Indicates the address of the secondary DNS server to be used by the PPP peer.
Message-Authenticator	Signs Access-Requests to prevent spoofing Access-Requests using CHAP, ARAP, or EAP authentication methods.
NAS-IP-Address	Indicates the identifying IP address of the NAS that is requesting authentication of the user, and must be unique to the NAS within the scope of the RADIUS server.
NAS-IPv6-Address	Indicates the identifying IPv6 Address of the NAS that is requesting authentication of the user, and must be unique to the NAS within the scope of the RADIUS server.
NAS-Identifier	Contains a string identifying the NAS originating the Access-Request.
NAS-Port	Indicates the physical port number of the NAS that is authenticating the user.
NAS-Port-Id	Contains a text string that identifies the port of the NAS that is authenticating the user.
NAS-Port-Type	Indicates the type of the physical port of the NAS that is authenticating the user.
Password-Retry	Indicates how many authentication attempts a user is allowed to attempt before being disconnected.
Port-Limit	Sets the maximum number of ports to be provided to the user by the NAS.
Prompt	Indicates to the NAS whether it should echo the user's response as it is entered, or not echo it.
Proxy-State	Indicates that a proxy server can send this attribute to another server when forwarding an Access-Request. The attribute must be returned unmodified in the Access-Accept, Access-Reject or Access-Challenge.
Reply-Message	Indicates that the text that can be displayed to the user.
Service-Type	Indicates the type of service the user has requested, or the type of service to be provided.

Attribute	Description
Session-Timeout	Sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt.
State	Indicates that the packet must have only zero or one State Attribute. Usage of the State Attribute is implementation dependent.
Telephone-number	Using the Calling-Station-Id and Called-Station-Id RADIUS attributes, authorization and subsequent tunnel attributes can be based on the phone number originating the call, or the number being called.
Termination-Action	Indicates the action the NAS should take when the specified service is completed.
Tunnel-Assignment-ID	Indicates to the tunnel initiator the particular tunnel to which a session is to be assigned.
Tunnel-Client-Auth-ID	Specifies the name used by the tunnel initiator during the authentication phase of tunnel establishment.
Tunnel-Client-Endpoint	Contains the address of the initiator end of the tunnel.
Tunnel-Link-Reject	Indicates the rejection of the establishment of a new link in an existing tunnel.
Tunnel-Link-Start	Marks the creation of a tunnel link.
Tunnel-Link-Stop	Marks the destruction of a tunnel link.
Tunnel-Medium-Type	Indicates the transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports.
Tunnel-Medium-Type	Indicates the transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports.
Tunnel-Password	Specifies a password used to access a remote server.
Tunnel-Preference	Indicates that if RADIUS server returns more than one set of tunneling attributes to the tunnel initiator, you should include this attribute in each set to indicate the relative preference assigned to each tunnel.
Tunnel-Private-Group-ID	Indicates the group ID for a particular tunneled session.

Attribute	Description
Tunnel-Reject	Marks the rejection of the establishment of a tunnel with another node.
Tunnel-Server-Auth-ID	Specifies the name used by the tunnel terminator during the authentication phase of tunnel establishment.
Tunnel-Server-Endpoint	Indicates the address of the server end of the tunnel.
Tunnel-Start	Marks the establishment of a tunnel with another node.
Tunnel-Stop	Marks the destruction of a tunnel to or from another node.
Tunnel-Type	Indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).
User-Name	Indicates the name of the user to be authenticated.
User-Password	Indicates the password of the user to be authenticated, or the user's input following an Access-Challenge.

Understanding RADIUS Accounting

You can configure the device to send session start and stop messages to a RADIUS accounting server. The device sends a user-session start message after the user successfully signs in and the device maps to a role.

Whenever a user session is terminated, the device sends a user-session stop message to the accounting server. A user session is terminated whenever the user:

- Manually signs out
- Times out because of either inactivity or exceeding the maximum session length
- Is denied access because of Host Checker role-level restrictions
- Is manually forced out by an administrator as a result of dynamic policy evaluation

If users are signed into a device cluster, the RADIUS accounting messages might show the users signing in to one node and signing out of another.

Table describes the attributes that are common to start and stop messages.

Attribute	Description
User-Name (1)	Specifies the string that the device administrator specifies during RADIUS server configuration.
NAS-IP-Address (4)	Specifies the device's IP address.
NAS-Port (5)	The device sets this attribute to 0 if the user signed in using an internal port, or 1 if an external port is used.
Framed-IP-Address (8)	Specifies the user's source IP address.
NAS-Identifier (32)	Specifies the configured name for the device client under the RADIUS server configuration.
Acct-Status-Type (40)	The device sets this attribute to 1 for a start message, or 2 for a stop message in a user-session or a subsession.
Acct-Session-Id (44)	Specifies the unique accounting ID that matches start and stop messages corresponding to a user-session or to a subsession.
Acct-Multi-Session-Id (50)	Specifies the unique accounting ID that you can use to link together multiple related sessions. Each linked session must have a unique Acct-Session-Id and the same Acct-Multi-Session-Id.
Acct-Link-Count (51)	Specifies the count of links in a multilink session at the time the system generates the accounting record.

Attribute	Description
Acct-Authentic (45)	<p>The device sets this attribute to:</p> <ul style="list-style-type: none"> • RADIUS—if the user is authenticated to a RADIUS server. • Local—if the user is authenticated to a local authentication server. • Remote—if the user is authenticated through any other RADIUS server.

Attribute	Description
Acct-Session-Time (46)	Specifies the duration of the user-session or the subsession.
Acct-Terminate-Cause (49)	The device uses one of the following values to specify the event that caused the termination of a user session or a subsession: <ul data-bbox="532 506 1263 741" style="list-style-type: none">• User Request (1) – User manually signs out.• Idle Timeout (4) – User is Idle and times out.• Session Timeout (5) – User’s maximum session times out.• Admin Reset (6) – User is forced out from active user’s page.

Interoperability Requirements and Limitations

You must configure the third-party RADIUS server to communicate with the Pulse Secure access management framework.

On the RADIUS server, configure the following settings:

- Hostname.
- Network IP address.
- Client type, if applicable. If this option is available, select Single Transaction Server or its equivalent.
- Type of encryption for authenticating client communication. This choice should correspond to the client type.
- Shared secret.

The following are the requirements and limitations for Interim update feature:

- If you want a server to receive interim accounting messages, you can statically configure an interim value on the client, in which case, the locally configured value overrides any value that might be included in the RADIUS Access-Accept message.
- The octet count reported in the accounting messages is the cumulative total since the beginning of the user session.

- The interim update byte count is only supported based on a user session, not on SAM or NC sessions.

Configuring Authentication with a RADIUS Server

To configure authentication with the RADIUS server:

1. Select **Authentication > Auth. Servers**.
2. Select **RADIUS Server** and click **New Server** to display the configuration page.
3. Complete the configuration as described below.
4. Save the configuration.

Auth Servers > IPv6-SBR-SRV

IPv6-SBR-SRV

Settings Users

*Name: Label to reference this server.

NAS-Identifier: Name of the device as known to RADIUS server

▼ Primary Server

*RADIUS Server: Name or IP address

*Authentication Port:

*Shared Secret:

*Accounting Port: Port used for RADIUS accounting, if applicable

NAS-IP-Address: IP address

*Timeout: seconds

*Retries:

Users authenticate using tokens or one-time passwords

▼ Backup Server (required only if Backup server exists)

RADIUS Server: Name or IP address

Authentication Port:

Shared Secret:

Accounting Port: Port used for RADIUS accounting, if applicable

Load-Balance Auth Requests between Primary and Backup Servers
Accounting requests will not be load-balanced.

▼ RADIUS accounting

User-Name: Template for reporting user identity to RADIUS server
The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. Click [here](#) to view a list of all variables.

Examples:
 <USER> The user's login name
 <REALM> The user's sign-in realm
 <ROLE SEP>"," The list of ","-separated roles assigned to the user
 <ROLE> The first role amongst multiple roles assigned to the user

Interim Update Interval: minutes Time interval to send an interim update to the accounting server (min: 15 minutes, max: 1440 minutes)

▼ Custom challenge expressions




Next Token:


New PIN:



Generic Login:

Save Changes Reset

Settings	Guidelines
Name	Specify a name to identify the server within the system.
NAS-Identifier	Specify the name that identifies the Network Access Server (NAS) client to the RADIUS server.

Settings	Guidelines
	<ul style="list-style-type: none"> - If you do not specify the NAS identifier, the value specified in the Hostname field on the System > Network > Overview page of the administrator console is used.  - If you use the RADIUS proxy feature, the NAS-Identifier field is not used. Proxy passes on the entire RADIUS packet including the NAS identifier from the client.
Primary Server	
Radius Server	Specify the name or IPv4/IPv6 address of the RADIUS server.
Authentication Port	Specify the authentication port value for the RADIUS server. Default port number: 1812, 1645 (legacy servers)
NAS-IP-Address	<p>Specify the NAS IP address.</p> <ul style="list-style-type: none"> - If you leave this field empty, the internal IP address is passed to RADIUS requests.  - If you configure the NAS IP address, then the system passes the value regardless of which cluster node sends the requests. - If you use the RADIUS proxy feature, this field is not used. - Proxy passes on the entire RADIUS packet including the NAS IP address from the client.
Timeout (seconds)	Specify the interval of time to wait for a response from the RADIUS server before timing out the connection.
Retries	Specify the number of times to try to make a connection after the first attempt fails.
Users authenticate using tokens or one-time passwords.	<p>Select this option to prompt the user for a token instead of a password. For example, you can use this option to dynamically prompt for a password or token based on sign-in policies by configuring two instances of the same authentication server. You can use one instance for wireless users with this option enabled and that prompts the user for a token, and another instance for wired users with this option disabled and that prompts the user for a password.</p> <p> If you are using RADIUS proxy feature, this option is not used.</p>
Backup Server (required only if Backup server exists)	

Settings	Guidelines
Radius Server	<p>Specify the secondary RADIUS server.</p> <p>The authentication request is first routed to the primary RADIUS server, then to the specified backup server if the primary server is unreachable.</p> <p>Accounting messages are sent to the RADIUS server by each cluster node without consolidation.</p> <p>RADIUS accounting follows these assumptions:</p> <ul style="list-style-type: none"> • If the cluster is active/passive, all users are connected to one node at a time. • If the cluster is active/active and does not use a balancer, users are connected to different nodes but are static. • If the cluster is active/active and uses a balancer, the balancer usually enforces a persistent source IP. In this case, users are always connected to the same node. <hr/> <p> RADIUS does not support load balancing.</p>
Authentication Port	Specify the authentication port.
Shared Secret	Specify the shared secret.
Accounting Port	Specify the accounting port.
Radius Accounting	
User-Name	<p>Specify the user information to the RADIUS accounting server.</p> <p>You can enter any of the applicable session variables. Applicable variables include those that are set the time after the user signs in and maps to a role. The default variables for this field are as follows:</p> <ul style="list-style-type: none"> • USER: Logs the username to the accounting server. • REALM: Logs the realm to the accounting server. • ROLE SEP=",";: Logs the list of comma-separated roles assigned to the user. • ROLE: Logs the role to the accounting server.

Settings	Guidelines
	<p> If you assign the user to more than one role, the system separates them with commas.</p>
Interim Update Interval (minutes)	<p>Select this option to achieve more precise billing for long-lived session clients and during network failure.</p> <ul style="list-style-type: none"> - If you are using the RADIUS proxy feature, the fields in this section are not used. - The minimum interim update interval is 15 minutes. The data statistics (bytes in and bytes out) for RADIUS accounting might not be sent for a J-SAM/W-SAM/NC session if the session is less than 30 seconds long and the applications keep the connections open all the time.
Custom challenge expressions	
<p>(Optional) Three types of challenge expressions exist with each automatically set to its pre-populated default. The custom option allows the administrator to configure the actual string pattern to match for any of the three modes. To add a custom expression, select the check box for the appropriate challenge expression type, and add a custom expression in the associated text box.</p> <ul style="list-style-type: none"> - If you use SecureID to authenticate users, then provide the user ID and the concatenation of PIN and the token value.  - When using CASQUE authentication, specify:([0-9a-zA-Z/+=] +): as the custom expression for the Generic Login Challenge Expression. - If you are using the RADIUS proxy feature, the fields in this section are not used. 	
Next Token	Specify the appropriate Next Token.
New PIN	Specify the New PIN.
Generic Login	Specify the Generic Login challenge to the user.

Using an ACE Server

This topic describes integration with an ACE Server (now named RSA Authentication Manager).

RSA Authentication Manager Overview

This section describes support for using IPS with an ACE Server (now named RSA Authentication Manager).

Understanding RSA Authentication Manager

[RSA Authentication Manager](#) (formerly known as ACE/Server) is an authentication and authorization server that allows user authentication based on credentials from the RSA SecurID® product from RSA Security Inc.

When you use RSA Authentication Manager as the authentication and authorization service for your Pulse Secure access management framework, users can sign in to IPS using the same username and password stored in the backend server.

Table describes RSA SecurID hardware token and software token user sign-in methods.

Method	Action
Using a hardware token and the standard system sign-in page	The user browses to the standard system sign-in page, and then enters the username and password (consisting of the concatenation of the PIN and the RSA SecurID hardware token's current value). The system then forwards the user's credentials to the authentication server.
Using a software token and the custom SoftID system sign-in page	The user browses to the SoftID custom sign-in page. Then, using the SoftID plug-in, the user enters the username and PIN. The SoftID plug-in generates a passphrase by concatenating the user's PIN and token and passes the passphrase to the authentication server.

If the RSA Authentication Manager positively authenticates the user, the user gains access to the system. Otherwise, the RSA Authentication Manager:

- Denies the user access to the system.
- Prompts the user to generate a new PIN (New PIN mode) if the user is signing in to the system for the first time. Users see different prompts depending on the method they use to sign in.
- If the user signs in using the SoftID plug-in, then the RSA prompts the user to create a new pin; otherwise IPS prompts the user to create a new PIN.

- Prompts the user to enter the next token (Next Token mode) if the token entered by the user is out of sync with the token expected by RSA Authentication Manager. Next Token mode is transparent to users signing in using a SoftID token. The RSA SecurID software passes the token through the system to RSA Authentication Manager without user interaction.
- Redirects the user to the standard system sign-in page (SoftID only) if the user tries to sign-in to the RSA SecurID Authentication page on a computer that does not have the SecurID software installed.

Feature Support

Pulse Secure access management framework supports the following RSA Authentication Manager features:

- New PIN mode
- Next-token mode
- Data Encryption Standard (DES)/ Secure Dial-In (SDI) encryption
- Advanced Encryption Standard (AES) encryption
- Slave Authentication Manager support
- Name locking
- Clustering

Interoperability Requirements and Limitations

The following limitations apply when defining and monitoring an RSA Authentication Manager instance:

- You can only add one RSA Authentication Manager configuration to the system, but you can use that configuration to authenticate any number of realms.
- You cannot customize the load balancing algorithm.
- When you enter the New PIN or Next Token mode, enter the required information within three minutes. Otherwise, the system cancels the transaction and notifies the user to reenter the credentials.



- The system can handle a maximum of 200 RSA Authentication Manager transactions at any given time. A transaction only lasts as long as is required to authenticate against the RSA Authentication Manager.

For example, when a user signs into the system, the RSA Authentication Manager transaction is initiated when the user submits the request for authentication and ends once the RSA Authentication Manager has finished processing the request. The user may then keep his or her session open, even though the RSA Authentication Manager transaction is closed.

Configuring Authentication with RSA Authentication Manager

To configure authentication with an ACE server:

1. Select **Authentication > Auth. Servers**.
2. Select **ACE Server** and click **New Server** to display the configuration page.
3. Complete the configuration as described in table.
4. Save the configuration.

Settings	Guidelines
Name	Specify a name to identify the server within the system.
ACE Port	Specify the default port of the authentication server.  If no port is specified in the sdconf.rec file, the default port is used.
Configuration File	
Current config file	Specify the RSA Authentication Manager configuration file.  You must update this file on the device anytime you make changes to the source file.

Settings	Guidelines
Imported on	Display the date on which the config file is imported.
Import new config file	Use the Choose File button to upload the sdconf.rec configuration file.
Node Verification File	
Node	Save the configuration to redisplay the configuration page. The updated page includes a section that lists a timestamp for the negotiation of the node secret between the system and the backend RSA server. The negotiation and verification automatically occurs after first successful log in. Do not expect entries in the table until at least one user has authenticated successfully.

Displaying the User Accounts Table

1. To display user accounts:
2. Select **Authentication > Auth. Servers**.
3. Click the link for the authentication server you want to manage.
4. Click the **Users** tab to display the user accounts table.

The user accounts table includes entries for the accounts that have been created. The Last Sign-in Statistic column shows the last successful sign-in date and time for each user, the user's IP address, and the agent or browser type and version.

Use the controls to search for users and manage user accounts:

- To search for a specific user, enter a username in the Show users named box and click **Update**.



You can use an asterisk (*) as a wildcard, where * represents any number of zero or more characters. For example, to search for all usernames that contain the letters jo, enter *jo*. The search is case-sensitive. To display the entire list of accounts again, type * or delete the field's contents and click **Update**.

- To limit the number of users displayed on the page, enter a number in the Show N users box and click Update.

- To terminate the user session and delete the account, select the check box next to the user account record and click Delete.

Using the SAML Server

This topic describes the local SAML authentication server. It includes the following information:

Overview

This section describes support for using the local SAML authentication server. It includes the following sections:

Understanding SAML

SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. The standard defines the XML-based assertions, protocols, bindings, and profiles used in communication between SAML entities. SAML is used primarily to implement Web browser single sign-on (SSO). SAML enables businesses to leverage an identity-based security system like Connect Secure to enforce secure access to web sites and other resources without prompting the user with more than one authentication challenge.

For complete details on the SAML standard, see the OASIS web site:

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

SAML Feature Support

When deployed as SAML service provider, IPS runs a local SAML server that relies on the SAML identity provider authentication and attribute assertions when users attempt to sign in to IPS. Note that authentication is only part of the IPS security system. The access management framework determines access to the system and protected resources.

IPS supports:

- HTTP Redirect binding for sending AuthnRequests
- HTTP Redirect binding for sending/receiving SingleLogout requests/responses
- HTTP POST and HTTP Artifact bindings for receiving SAML responses
- RequestedAuthnContext context class specifications



IPS currently supports SAML server as Service Provider and IPS as SAML Identity Provider (IdP) is not supported.

Interoperability Requirements and Limitations

Before you begin:

- Check to see whether the SAML identity provider implements SAML 2.0 or SAML 1.1.
- Check to see whether the SAML identity provider uses HTTP POST or HTTP Artifact bindings for SAML assertions.
- Check to see whether the SAML identity provider has published a SAML metadata file that defines its configuration. If the SAML identity provider metadata file is available, configuration is simpler and less prone to error.
- Complete the system-wide SAML settings if you have not already done so. Select **System > Configuration > SAML > Settings**. For details, see [Configuring Global SAML Settings](#)
- Add metadata for the SAML identity provider to the metadata provider list if you have not already done so. Select **System > Configuration > SAML**. For details, see [Managing SAML Metadata Files](#).

The sign-in URL for which a session needs to be established for Connect Secure as a service provider is identified by the RelayState parameter (HTTP URL parameter for artifact and HTML form parameter for POST.) In a service provider initiated case, the system populates RelayState as an HTTP URL parameter while sending AuthnRequest. In the IdP-Initiated scenario (Connect Secure is a service provider and there is a third-party IdP), the IdP must be configured to set the appropriate Sign-in URL of Connect Secure in the RelayState parameter of the HTML form containing the SAML response. For more information, see [SAML Feature Support](#).



Configuring Authentication with the SAML Server

To configure the SAML server:

1. Select **Authentication > Auth. Servers**.
2. Select **SAML Server** and click **New Server** to display the configuration page.

3. Complete the configuration as described in table.
4. Save the configuration.

Settings	Guidelines
Name	Specify a name to identify the server instance.
Settings	
SAML Version	Select 2.0 or 1.1, depending on the SAML version used by the SAML IdP.
Policy Secure Entity Id	This value is prepopulated. It is generated by the system, based on the value for the Host FQDN for SAML setting on the System > Configuration > SAML > Settings page.
Configuration Mode	Select Manual or Metadata. If a metadata file or location is available from the SAML identity provider, use the metadata option to make configuration simpler and less prone to error. To upload or set the location for the published metadata file, select System > Configuration > SAML and click the New Metadata Provider button.
Identity Provider Entity ID	<p>The identity provider entity ID is sent as the Issuer value in the assertion generated by the SAML identity provider.</p> <p>If you use the metadata option, this setting can be completed by selecting the identity provider entity ID from the list. The list is populated by the identity provider entities defined in metadata files added to the System > Configuration > SAML page.</p> <p>If you complete this setting manually, specify the Issuer value in assertions generated by the SAML identity provider. Typically, you ask the SAML identity provider administrator for this setting.</p>
Identity Provider Single Sign On Service URL	<p>The identity provider SSO service URL is a URL provisioned by the SAML identity provider. The setting is required to support service-provider-initiated SSO. If missing, the system cannot successfully redirect the user request.</p> <p>If you use the metadata option, this setting can be completed by selecting the SSO service URL from the list. The list is populated by the identity provider entities defined in metadata files added to the System > Configuration > SAML page.</p> <p>If you complete this setting manually, ask the SAML identity provider administrator for this setting.</p>

Settings	Guidelines
User Name Template	<p>Specify how the system is to derive the username from the assertion. If the field is left blank, it uses the string received in the NameID field of the incoming assertion as the username.</p> <p>If you choose a certificate attribute with more than one value, the system uses the first matched value. For example, if you enter <certDN.OU> and the user has two values for the attribute (ou=management, ou=sales), the system uses "management". To use all values, add the SEP attribute to the variable. For example, if you enter <certDN.OUT SEP=":">, the system uses "management:sales". The attributes received in the attribute statement in the incoming assertion are saved under userAttr. These variables can also be used with angle brackets and plain text. If the username cannot be generated using the specified template, the login fails. If the NameID field of the incoming assertion is of type X509Nameformat, then the individual fields can be extracted using system variable "assertionNameDN".</p> <hr/> <p> Currently supported NameIDs are - EMAIL, X509_SUBJECT, WIN_DOMAIN_QUALIFIED. If a SAML request is received with a different NameID format, then processing of the request fails with unsupported NameID format error message.</p>
Allowed Clock Skew (minutes)	<p>Specify the maximum allowed difference in time between the system clock and the SAML identity provider server clock.</p> <hr/> <p> SAML is a time sensitive protocol. The time-based validity of a SAML assertion is determined by the SAML identity provider. If the SAML identity provider and SAML service provider clocks are askew, the assertion can be determined invalid, and you will receive the following error:</p> <hr/> <p>"SAML Transferred failed. Please contact your system administrator. Detail: Failure: No valid assertion found in SAML response."</p> <p>Ensure that the clocks are synchronized using NTP server and that you set an Allowed Clock Skew value that accommodates any expected or permissible skew.</p>
Support Single Logout	<p>Single logout is a mechanism provided by SAML for logging out a particular user from all the sessions created by the identity provider. Select this option if the system must receive and send a single logout request for the peer SAML identity provider.</p>

Settings	Guidelines
	<p>If you use the metadata option, the Single Logout Service URL setting can be completed by selecting the SLO service URL from the list. The list is populated by the identity provider entities defined in metadata files added to the System > Configuration > SAML page. The system sends Single Logout requests to this URL.</p> <p>In addition, if you use the metadata option, the Single Logout Response URL setting is completed based on your selection for Single Logout Service URL. If the identity provider has left this setting empty in its metadata file, the system sends the Single Logout response to the SLO service URL.</p> <p>If you complete these settings manually, ask the SAML identity provider administrator for guidance.</p> <p>The Support Single Logout service for the identity provider must present a valid certificate.</p> <p>This feature is supported with Pulse Desktop Client beginning with Release 9.1R9.</p>
SSO Method	
Artifact	<p>When configured to use the Artifact binding, the system contacts the Artifact Resolution Service (ARS) to fetch the assertion using SOAP protocol. If the ARS is hosted on a HTTPS URL, then the certificate presented by the ARS is verified by the system. For this verification to pass successfully, the CA of the server certificate issued to the identity provider ARS must be added to the trusted server CA on the system.</p> <p>Complete the following settings to configure SAML using the HTTP Artifact binding:</p> <ul style="list-style-type: none"> • Source ID. Enter the source ID for the identity provider ARS. Source ID is Base64-encoded, 20-byte identifier for the identity provider ARS. If left blank, this value is generated by the system. • Source Artifact Resolution Service URL. For metadata-based configuration, this field is completed automatically from the metadata file and is not configurable. For manual configurations, enter the URL of the service to which the SP ACS is to send ArtifactResolve requests. ArtifactResolve requests are used to fetch the assertion from the artifact received by it.

Settings	Guidelines
	<ul style="list-style-type: none"> • SOAP Client Authentication. Select HTTP Basic or SSL Client Certificate and complete the related settings. If you use an SSL client certificate, select a certificate from the device certificate list. • Select Device Certificate for Signing. Select the device certificate the system uses to sign the AuthnRequest sent to the identity provider SSO service. If you do not select a certificate, the system does not sign AuthnRequest. • Select Device Certificate for Encryption. Select the device certificate the system uses to decrypt encrypted data received in the SAML response. The public key associated with the device certificate is used by the identity provider for encryption.
POST	<p>When configured to use the POST binding, the system uses a response signing certificate to verify the signature in the incoming response or assertion. The certificate file must be in PEM or DER format. The certificate you select should be the same certificate used by the identity provider to sign SAML responses. Complete the following settings to configure SAML using the HTTP POST binding:</p> <ul style="list-style-type: none"> • Response Signing Certificate. If you use the metadata-based configuration option, select a certificate from the list. The list is populated by the identity provider entities defined in metadata files added to the System > Configuration > SAML page. <p>If you configure these settings manually, browse to and upload the certificate to be used to validate the signature in the incoming response or assertion. If no certificate is specified, the certificate embedded in the response is used.</p> <ul style="list-style-type: none"> • Enable Signing Certificate status checking. Select this option to check the validity of the signing certificate before verifying the signature. This setting applies to any certificate used for signature verification. If this option is enabled, the response will be rejected if the certificate is revoked, expired, or untrusted. If this option is selected, the certificate CA must be added to the Trusted Client CA store. <p>If this option is not enabled, then the certificate is used without any checks.</p>

Settings	Guidelines
	<ul style="list-style-type: none"> • Select Device Certificate for Signing. Select the device certificate the system uses to sign the AuthnRequest sent to the identity provider SSO service. If you do not select a certificate, the system does not sign AuthnRequest. • Select Device Certificate for Encryption. Select the device certificate the system uses to decrypt encrypted data received in the SAML response. The public key associated with the device certificate is used by the identity provider for encryption.
Authentication Context Classes	<p>Use the Add and Remove buttons to select authentication context classes to be sent in the authentication requests to the SAML identity provider. These are included in the RequestedAuthnContext element.</p> <p>In the OASIS standard, an authentication context is defined as "the information, additional to the authentication assertion itself, that the relying party may require before it makes an entitlements decision with respect to an authentication assertion."</p> <p>This feature supports all authentication context classes specified in the SAML 2.0 OASIS Authn Context specification</p> <p>For example, if you select X509, the system sends the following context:</p> <pre><samlp:RequestedAuthnContext> <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"> urn:oasis:names:tc:SAML:2.0:ac:classes:X509</saml:AuthnContextClassRef> </samlp:RequestedAuthnContext></pre> <p>In response, the SAML IdP sends the context data along with the authentication results. The system stores the context data in the session cache and as a system variable named samlAuthnContextClass. The system variable can be used in role mapping rules and resource policy detailed rules.</p> <p>Specify a comparison attribute within the RequestedAuthnContext element. The comparison attribute specifies the relative strengths of the authentication context classes specified in the request and the authentication methods offered by a SAML IdP. The following values defined in the SAML 2.0 OASIS core specification can be selected:</p>

Settings	Guidelines
	<ul style="list-style-type: none"> • exact—Requires the resulting authentication context in the authentication statement to be the exact match of at least one of the authentication contexts specified. • minimum—Requires the resulting authentication context in the authentication statement to be at least as strong as one of the authentication contexts specified. • maximum—Requires the resulting authentication context in the authentication statement to be stronger than any one of the authentication contexts specified. • better—Requires the resulting authentication context in the authentication statement to be as strong as possible without exceeding the strength of at least one of the authentication contexts specified. <p>Select the same value that is configured on the SAML IdP. If none is specified in the SAML IdP configuration, the implicit default is exact.</p>
Service Provider Metadata Settings	
Metadata Validity	Enter the number of days the metadata is valid. Valid values are 0 to 9999. 0 specifies the metadata does not expire.
Do Not Publish IPS Metadata	Select this option if you do not want to publish the metadata at the location specified by the Entity ID field.
Download Metadata	This button appears only after you have saved the authentication server configuration. Use this button to download the metadata of the current SAML service provider.

Displaying the User Accounts Table

To display user accounts, refer to the steps found in [Displaying the User Accounts Table](#).

Access Control with SAML Server

In a SAML deployment, a SAML service provider is configured to request authentication from a SAML identity provider. The SAML identity provider responds with assertions regarding the identity, attributes, and entitlements (according to your configuration). The exchange enforces security and enables the SSO user experience.

IPS as a SAML Service Provider

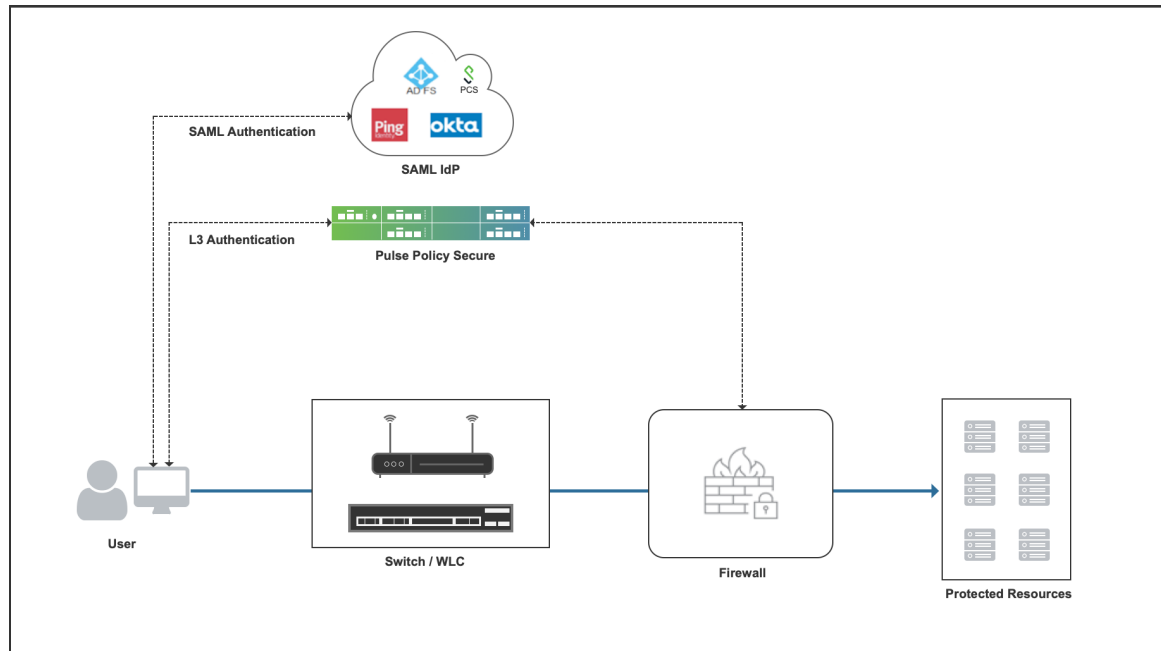
If you are working with a partner that has implemented a SAML identity provider, you can deploy the IPS as a SAML service provider to inter-operate with it, thereby enabling SSO for users who should have access to protected resources. In this model, the user is authenticated by the SAML identity provider. The system uses the SAML response containing the assertion to make an authentication decision.

The choices the identity provider makes to implement SAML determine the deployment choices, for example whether to use SAML 2.0 or SAML 1.1, whether to reference a published metadata configuration file, and whether to use a POST or artifact profile. When you deploy the system as a SAML service provider, you create a SAML authentication server configuration that references the partner SAML identity provider, and a set of access management framework objects (realm, role mapping rules, and sign-in policy) that reference the SAML authentication server.

Layer 3 Authentication and Enforcement using SAML Server

Figure shows how to access firewall protected resources using SAML server on IPS.

1. End user using a user agent (either a browser or a Pulse client) authenticates to IPS



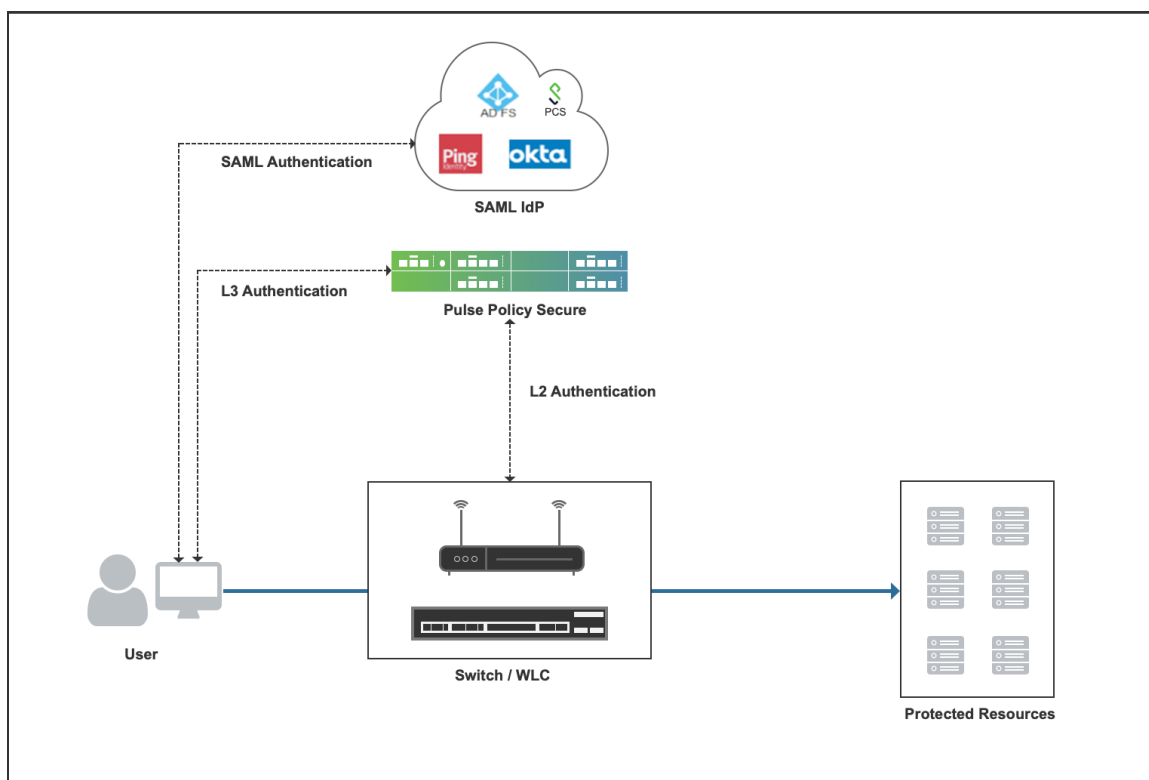
2. Ivanti Policy Secure(IPS) acting as a SAML Service Provider (SP), issues a SAML authentication (SAML AuthN) request to SAML IdP through the user agent. If SAML authentication request is valid, IdP authenticates the end user and generates SAML assertion and sends it to IPS (SAML SP) through user agent.
3. Ivanti Policy Secure(IPS) validates the SAML assertion and if it's valid, authentication is successful.
4. The user is first authenticated with SAML IdP. Once end user is authenticated appropriate role is assigned and the user ID is pushed to firewall. The end user can access the protected resource.



Pulse Client uses embedded browser for SAML authentication. It should be enabled on the Pulse Client connection settings in IPS.

Layer 2 Authentication and Enforcement using SAML Server

Figure shows how to access switch protected resources using SAML server on IPS.



For Layer 2 access control using SAML server on IPS, below mechanism is used:

1. MAC address authentication is performed using either RADIUS or SNMP for Layer 2 authentication. The session is created on IPS after successful MAC authentication and the user is provided with a limited access role since the Host Checker is not performed.
2. The user must be able to access both IPS and SAML IdP after L2 authentication. For policy enforcement using MAC address authentication, see here.
3. Pulse Client or web browser is used to perform Layer 3 authentication using SAML server.
4. After successful Layer 3 authentication on IPS via SAML IdP, both Layer 2 (MAC authentication) and Layer 3 (SAML authentication) connections are bridged using MAC address.
5. Host Checker is performed and if the SAML authentication is successful the user is provided with Full Access Role.
6. The user can access protected resources.



Layer 2 session is updated with the RADIUS attributes of the Layer 3 connection. The bridged session is used to perform Layer 2 access control. For more information on session bridging, see [here](#).

SAML 2.0 Configuration Tasks

To use SAML server on IPS follow the below configuration steps:

Configure SAML host FQDN under Configuration > SAML > Settings. This FQDN is used to generate SAML Entity Id. See [Configuring System-Wide SAML Settings](#)

Configure third party

SAML IdP like Ping Federate, Okta. Get SAML IdP metadata and configure it under Configuration > SAML > New Metadata Provider. Under Metadata Provider configuration, "Identity Provider" roles should be selected since it is an SAML IdP metadata. (For screenshot, refer section "Admin UI changes")

Configure SAML Server under

1. Authentication > Auth. Server. See [Configuring SAML Authentication server](#).
 - If SAML IdP's metadata is not configured, admin needs to configure IdP's information manually.
 - If only one IdP metadata is configured, IdP information is automatically populated. If multiple IdP metadata are configured, admin needs to selected appropriate IdP's information.
 - If admin wants to sign or encrypt the request, appropriate certificates need to be selected.

After configuring SAML server on IPS, the metadata of IPS acting as an SAML SP can be downloaded from SAML server page.

Configure IPS metadata on SAML IdP and configured SAML SP details on IdP. See [Configuring IPS as a SAML 2.0 Service Provider](#)

Configuring System-Wide SAML Settings

This section describes tasks related to configuring system-wide SAML settings. It includes the following topics:

Configuring Global SAML Settings

The system-wide SAML settings impact all SAML service provider and identity provider instances.

To configure global SAML settings:

1. Select **System > Configuration > SAML**.
2. Click the **Settings button** to display the configuration page.
3. Complete the settings described in
4. Click Save Changes.

SAML >
Settings

▼ Metadata Server Configuration

Timeout value for metadata fetch request: seconds 1 - 600. Specifies the time in seconds to wait for response of SAML metadata fetch request.

Validity of uploaded/downloaded metadata file: days 0 - 9999. Specifies the time in days after which downloaded/uploaded metadata file expires. 0 means that Policy Secure doesnot enforce any validity on the peer metadata file

Host FQDN for SAML: The FQDN used for generating URLs for SAML services.

Settings	Guidelines
Timeout value for metadata fetch request	Specify the number of seconds after which a download request is abandoned. If the peer SAML entity publishes its metadata at a remote location, the system downloads the metadata file from the specified location.
Validity of uploaded/downloaded metadata file	Specify the maximum duration for which the system considers the metadata file of the peer SAML entity to be valid. If the metadata file provided by the peer SAML entity contains validity information, the lower value takes precedence.
Host FQDN for SAML	Specify the fully qualified domain name for the Connect Secure host. The value you specify here is used in the SAML entity ID and the URLs for SAML services, including: <ul style="list-style-type: none"> • Entity ID for SAML service provider and SAML identity provider instances. The SAML entity ID is the URL where the system publishes its SAML metadata file. • Single sign-on service URL

Settings	Guidelines
	<ul style="list-style-type: none">• Single logout service URL• Assertion consumer service URL• Artifact resolution service URL <p>BEST PRACTICE: The system uses HTTPS for these services. It is recommend to assign a valid certificate to the interface that has the IP address to which this FQDN resolves so that users do not see invalid certificate warnings.</p>

Managing SAML Metadata Files

You use the System > Configuration > SAML pages to maintain a table of SAML metadata files for the SAML service providers and identity providers in your network. Using SAML metadata files makes configuration easier and less prone to error.

You can add the metadata files to the system by:

- Uploading a metadata file.
- Retrieving the metadata file from a well-known URL.

To add metadata files:

1. Select **System > Configuration > SAML**.
2. Click **New Metadata Provider** to display the configuration page.
3. Complete the settings described in table.

4. Save the configuration.

New Metadata Provider

Name: Label to reference metadata provider.

Metadata Provider Location Configuration

Location: Local Remote. Location of metadata provider. In case of Local, metadata file needs to be uploaded by admin. In case of Remote Location, metadata file is fetched by Policy Secure from the configured download url.

Upload Metadata File: No file chosen
Current File: None

Metadata Provider Verification Configuration

Accept Unsigned Metadata. If checked Policy Secure accepts unsigned metadata.

Signing Certificate: Issued To:
Issued By:
Valid:
Details:

Upload Certificate: No file chosen
 Enable Signing Certificate status checking
(When configured in Trusted Client CA. This applies to the certificate configured above as well as the one comes along with the Metadata.)

Metadata Provider Filter Configuration

Roles: Identify Provider Service Provider Policy Decision Point. Roles which Policy Secure looks for in the metadata file.
List of entity ids to be imported. (one per line). If left empty all entity ids in the file are imported.

Entity ids to import:

Settings	Guidelines
Metadata Provider Location Configuration	<p>Select one of the following methods:</p> <ul style="list-style-type: none"> Local. Browse and locate the metadata file on your local host or file system. Remote. Enter the URL of the metadata file. Only http and https protocols are supported.
Metadata Provider Verification Configuration	
Accept Untrusted Server Certificate	If you specify a URL for the metadata provider, select this option to allow the system to download the metadata file even if the server certificate is not trusted. This is necessary only for HTTPS URLs.
Accept Unsigned Metadata	If this option is not selected, unsigned metadata is not imported. Signed metadata is imported only after signature verification.
Signing Certificate	Browse and locate the certificate that verifies the signature in the metadata file. This certificate overrides the certificate specified in the signature of the received metadata. If no certificate is uploaded here, then the certificate present in the signature of the received metadata is used.

Settings	Guidelines
	Select the Enable Certificate Status Checking option to verify the certificate before using it. Certificate verification applies both to the certificate specified here and the certificate specified in the signature in the metadata file.
Metadata Provider Filter Configuration	
Roles	Select whether the metadata file includes configuration details for a SAML service provider, identity provider, or Policy Decision Point. You may select more than one. If you select a role that is not in the metadata file, it is ignored. If none of the selected roles are present in the metadata file, the system returns an error.
Entity IDs To Import	Enter the SAML Entity IDs to import from the metadata files. Enter only one ID per line. Leave this field blank to import all IDs. This option is available only for uploading local metadata files.

The Refresh button downloads the metadata files from the remote location even if these files have not been modified. This operation applies only to remote locations; local metadata providers are ignored if selected.

To refresh a metadata file:

1. Select **System > Configuration > SAML**.
2. Select the metadata file to refresh and click Refresh.

To delete a metadata file:

1. Select **System > Configuration > SAML**.
2. Select the metadata file to delete and click **Delete**.

Configuring IPS as a SAML 2.0 Service Provider

This topic describes how to configure the system as a SAML service provider. When the system is a SAML service provider, it relies on the SAML identity provider authentication and attribute assertions when users attempt to sign in to the device. Note that authentication is only part of the security system. The access management framework determines access to the system and protected resources.

The system supports:

- HTTP Redirect binding for sending AuthnRequests
- HTTP Redirect binding for sending/receiving SingleLogout requests/responses
- HTTP POST and HTTP Artifact bindings for receiving SAML responses
- RequestedAuthnContext context class specifications

Before you begin:

- Check to see whether the SAML identity provider uses HTTP POST or HTTP Artifact bindings for SAML assertions.
- Check to see whether the SAML identity provider has published a SAML metadata file that defines its configuration. If the SAML identity provider metadata file is available, configuration is simpler and less prone to error.
- Complete the system-wide SAML settings if you have not already done so. Select System > Configuration > SAML > Settings. For details, see [Configuring Global SAML Settings](#)
- Add metadata for the SAML identity provider to the metadata provider list if you have not already done so. Select System > Configuration > SAML. For details, see [Managing SAML Metadata Files](#)

The sign-in URL for which a session needs to be established for the system as a service provider is identified by the RelayState parameter (HTTP URL parameter for artifact and HTML form parameter for POST.) In a service provider initiated case, the system populates RelayState as an HTTP URL parameter while sending AuthnRequest. In the IdP-Initiated scenario (Connect Secure is a service provider and there is a third-party IdP), the IdP must be configured to set the appropriate Sign-in URL of the system in the RelayState parameter of the HTML form containing the SAML response. For more information, see the SAML 2.0 specification.

To configure the system as a SAML service provider:

1. Select **Authentication > Auth. Servers**.
2. Select **SAML Server** from the New list and then click **New Server** to display the configuration page.
3. Complete the settings as described in table.
4. Save the configuration.

After you save changes for the first time, the page is redisplayed and now has two tabs. Use the Settings tab to modify any of the settings pertaining to the SAML server configuration. Use the Users tab to monitor user sessions.

Next steps:

- Configure the access management framework to use the SAML authentication server. Start with realm and role mapping rules.
- Configure a sign-in policy. When using a SAML authentication server, the sign-in policy can map to a single realm only.

Configuring a Role Mapping Rule Based on a SAML Attribute

You can use role mapping rule custom expressions to include SAML Attribute statement as a factor in role determination. IPS uses attributes from attribute statement in "User Name Template" under **Authentication > Auth. Server > SAML Server**.

To configure role mapping rules:

1. Select **Users > User Realms**.
2. Create a new realm or edit a realm you have already created.
3. Click New Rule to display the configuration page.
4. Select **Custom Expression** and click **Update** to redisplay the configuration page with the controls related to custom expressions.

- Click **Expressions** to display the server catalog dialog box.

The screenshot shows a configuration interface with two tabs: 'Expressions' (selected) and 'Variables'. Under 'Expressions', there is a 'View' dropdown menu set to 'saml'. Below it, a 'Name' text box contains 'saml'. A larger 'Expression' text area contains the text `userAttr.group = "engg"`. To the right, an 'Expressions Dictionary' list shows various attributes with expandable arrows. At the bottom, there are three buttons: 'Save Changes', 'Close', and 'Delete'. Below these is a small dropdown menu and a blue button labeled '< Insert Expression'.

On SAML IdP, attributes in attribute statement can be configured as name-value pairs and/or can be fetched from directory server. For example, an attribute with name="group" and value="engg" can be configured on IdP asserts that an authenticated user belongs to engineering group. SAML assertion from IdP contains this attribute in attribute statement.

- Select `samlAuthnContextClass`, select an operator, and click Insert Expression.
- Edit the expression template to match the `AuthnContextClassRef` data expected from the SAML IdP.
- Save your changes to the variable expression and return to the rule configuration page.
- Select the expression, roles for the rule, and the stop option (if desired).
- Save your changes to the rule configuration and return to the realm configuration page.
- Reorder the rules if necessary.
- Save the realm configuration.

Using a SiteMinder Server

This topic describes integration with the SiteMinder server.

SiteMinder Server Overview

This section describes support for using IPS with the SiteMinder server.

Understanding SiteMinder Server

CA SiteMinder server is an authentication and authorization server.

When you configure the Pulse Secure access management framework to authenticate users with a SiteMinder policy server, the system passes the user's credentials to SiteMinder during authentication. Once SiteMinder receives the credentials, it may use standard username and password authentication, RSA Authentication Manager SecurID tokens, or client-side certificates to authenticate the credentials.

The system also passes a protected resource URL to SiteMinder during authentication to determine which SiteMinder realm it should use to authenticate the user. When the system passes the protected resource URL, SiteMinder authorizes the user's URL against the realm that is associated with the resource and allows the user to seamlessly access any resources whose protection levels are equal to or less than the URL that was passed.

Feature Support

The Pulse Secure access management framework supports the following SiteMinder features:

Single Sign-on Using SMSESSION Cookies

The Pulse Secure access management framework enables single sign-on (SSO) to SiteMinder-protected resources using SMSESSION cookies. An SMSESSION cookie is a security token that encapsulates SiteMinder session information. Depending on your configuration, either the SiteMinder Web agent or the system creates an SMSESSION cookie and then posts the cookie to the following locations so the user does not have to reauthenticate to access additional resources.

- Pulse Secure access management framework-If the user tries to access a SiteMinder resource within the session (for example, from the system file browsing page), the system passes its cached SMSESSION cookie to the Web agent for authentication.

- The user's Web browser-If the user tries to access a SiteMinder resource from outside the session (for example, when using a protected resource on a standard agent), SiteMinder uses the cached SMSESSION cookie stored in the user's Web browser to authenticate/authorize the user.

Automatic Sign-In

If you enable the Automatic Sign-In option, the system can use an SMSESSION cookie generated by another agent to enable single sign-on from a SiteMinder resource. When a user accesses the system sign-in page with an SMSESSION cookie, the system verifies the SMSESSION cookie. Upon successful verification, the system establishes a session for the user. You can use the following authentication mechanisms when you enable automatic sign-in through the system:

- Custom agent-The system authenticates the user against the policy server and generates a SMSESSION cookie. When you select this option, you can enable SSO on other SiteMinder agents that use the same policy server. To enable SSO on these agents, update each of them to accept third-party cookies. If you select this option and the user enters his system session with an SMSESSION cookie, the system attempts automatic sign-in when the user enters the session.
- HTML form post-The system posts credentials to a standard Web agent that you have already configured. The Web agent then creates SMSESSION cookies. If you select this option, you cannot use SecurID New Pin and Next Token modes or client-side certificate authentication. If you select this option and the user enters his session with an SMSESSION cookie, the system attempts automatic sign-in when the user enters the session.
- Delegated authentication-The system delegates authentication to a standard agent. If this option is enabled, the system tries to determine the FCC URL associated with the protected resource. The system then redirects the user to the FCC URL with the system sign-in URL as the target. Upon successful authentication, the user is redirected back to the system with an SMSESSION cookie and the system does an automatic sign-in for the user.

Authentication Schemes

The Pulse Secure access management framework works with the following types of SiteMinder authentication schemes:

- **Basic username and password authentication**—The user's name and password are passed to the SiteMinder policy server. The policy server authenticates them to another server for authentication.

- **RSA Authentication Manager SecurID token authentication**—The SiteMinder policy server authenticates users based on a username and password generated by an RSA Authentication Manager SecurID token.
- **Client-side certificate authentication**—The SiteMinder policy server authenticates users based on their client-side certificate credentials. If you choose this authentication method, the Web browser displays a list of client certificates from which users can select. If you choose to authenticate users with this method, you must import the client certificate through the **System > Certificates > Trusted Client CAs** tab.

Interoperability Requirements and Limitations

The following requirements and limitations apply:

- The Automatic Sign-in feature is not supported for administrator roles. This feature is only available for end users.
- If you use the Authenticate using custom agent option, update all other Web agents to accept the device generated cookie, and apply a software patch to all other Web agents.
- Ivanti Policy Secure(IPS) supports SiteMinder server version 6.0, version 5.5, and version 12.0. If you run older agents than the supported agents, you might experience cookie validation problems, including crossed log entries and intermittent user timeouts.
- You can choose which SiteMinder server version you want to support when you create a server instance. You can choose version 5.5, which supports both versions 5.5 and 6.0, or you can choose version 6.0, which supports only version 6.0, or version 12.0. There is no difference in the SiteMinder authentication server functionality based on which version you select. This option only controls the version of the SDK to use. We recommend you match the compatibility mode with the version of the policy server.
- When you use SiteMinder to authenticate, the primary and backup policy servers must run the same SiteMinder server software version. A mixed deployment (where the primary server runs a different server software version than the backup) is not supported.
- SiteMinder does not store the IP address in the SMSESSION cookie, and therefore cannot pass it to the system.
- SiteMinder sends the SMSESSION cookie to the system as a persistent cookie. To maximize security, the system resets the persistent cookie as a session cookie once authentication is complete.

- When you use SiteMinder to authenticate, the Pulse Secure access management framework disregards any system session and idle timeouts and uses session and idle timeouts set through the SiteMinder realm instead.
- When you use SiteMinder to authenticate, users must access the system using a fully qualified domain name. This is because the SiteMinder SMSESSION cookie is only sent for the domain for which it is configured. If users access the system using an IP address, they might receive an authentication failure and will be prompted to authenticate again.
- You can update all your standard Web agents to the appropriate SiteMinder Agent Quarterly Maintenance Release (QMR) to accept the cookies. If you are running SiteMinder version 5 Web agents, use the QMR5 hot fix. The system is compatible with version 5.x and later SiteMinder agents. Older versions of SiteMinder agents are susceptible to cookie validation failures.
- You can set the Accept Third Party Cookie attribute (AcceptTPCookie) to yes in the Web agent's configuration file (webagent.conf) or to 1 in the Windows Registry for the IIS Web server. The location of the attribute depends on the SiteMinder version and Web server you are using. Refer to the documentation provided with your SiteMinder server.

Configuring the Back-End SiteMinder Server

The following sections do not give complete SiteMinder configuration instructions—they are only intended to help you make SiteMinder work with the Pulse Secure access management framework. For in-depth SiteMinder configuration information, refer to the documentation provided with your SiteMinder policy server.

Configuring the SiteMinder Agent

A SiteMinder agent filters user requests to enforce access controls. For instance, when a user requests a protected resource, the agent prompts the user for credentials based on an authentication scheme and sends the credentials to a SiteMinder policy server. A Web agent is simply an agent that works with a Web server. When configuring SiteMinder to work with the Pulse Secure access management framework, you must configure the system as a Web agent in most cases.

If you select the Delegate authentication to a standard agent option, you must set the following options in the agent configuration object of the standard Web agent to host the FCC URL:

- <EncryptAgentName=no>
- <FCCCompatMode=no>

To configure the system as a Web agent on the SiteMinder policy server:

1. In the SiteMinder Administration interface, click the System tab.
2. Right-click Agents and select Create Agent.
3. Enter a name for the Web agent and a description. You must enter this name when creating a SiteMinder realm.
4. Select the Support 5.x agents option for compatibility with the system.
5. Under Agent Type, select SiteMinder and then select Web Agent from the list. This setting is required for compatibility with the system.
6. Under IP Address or Hostname, enter the name or IP address of the system.
7. In the Shared Secret box, enter and confirm a secret for the Web agent. Note that you must enter this secret when configuring the system.
8. Click **OK**.

Configuring the Authentication Scheme

Within SiteMinder, an authentication scheme is a way to collect user credentials and determine the identity of a user. You may create different authentication schemes and associate different protection levels with each. For example, you may create two schemes—one that authenticates users based solely on the users' client-side certificates and provides them a low protection level, and a second that uses RSA Authentication Manager SecurID token authentication and provides users a higher protection level.

To configure a SiteMinder authentication scheme:

1. In the SiteMinder Administration interface, select the System tab. Right-click Authentication Schemes and select Create Authentication Scheme.
2. Enter a name for the scheme and (optionally) a description. You must enter this name when configuring the SiteMinder realm.

3. Under Authentication Scheme, select one of the following options:
 - Basic Template
 - HTML Form Template
 - SecurID HTML Form Template-If you are using SecurID authentication, you must choose SecurID HTML Form Template (instead of SecurID Template). Choosing this option enables the Policy Server to send ACE sign-in failure codes.
 - X509 Client Cert Template
 - X509 Client Cert and Basic Authentication



- You must select HTML Form Template to handle reauthentication.
 - If you select X509 Client Cert Template or X509 Client Cert and Basic Authentication, you must import the certificate through System > Certificates > Trusted Client CAs.
-

4. Enter a protection level for the scheme. Note that this protection level carries over to the SiteMinder realm that you associate with this scheme.
5. Select Password Policies Enabled for this Authentication Scheme if you want to reauthenticate users who request resources with a higher protection level than they are authorized to access.
6. Select Scheme Setup tab, and enter the options required by your authentication scheme type.
7. If you want the system to reauthenticate users who request resources with a higher protection level than they are authorized to access, you must enter the following settings:
 - Under Server Name, enter the hostname (for example, sales.yourcompany.net).
 - Select the Use SSL Connection check box.
 - Under Target, enter the sign-in URL defined plus the parameter "ive=1" (for example, /highproturl?ive=1). The system must have a sign-in policy that uses */highproturl as the sign-in URL and only uses the corresponding SiteMinder authentication realm.
 - Clear the Allow Form Authentication Scheme to Save Credentials check box.
 - Leave Additional Attribute List empty.
8. Click **OK**.

If you change a SiteMinder authentication scheme on the policy server, you must flush the cache using the Flush Cache option on the Advanced tab.

Configuring the SiteMinder Domain

Within SiteMinder, a policy domain is a logical grouping of resources associated with one or more user directories. Policy domains contain realms, responses, and policies. When configuring the Pulse Secure access management framework to work with SiteMinder, you must give user access to a SiteMinder resource within a realm, and then group the realm into a domain.

To configure a SiteMinder domain

1. Select the System tab, right-click Domains and select Create Domain, or click Domains and select an existing SiteMinder domain.
2. Add a realm to the domain.

Configuring the SiteMinder Realm

Within SiteMinder, a realm is a cluster of resources within a policy domain grouped together according to security requirements. When configuring SiteMinder to work with the Pulse Secure access management framework, you must define realms to determine which resources the users might access.

To configure a SiteMinder Realm:

1. In the SiteMinder Administration interface, In the SiteMinder Administration interface, select the Domains tab.
2. Expand the domain that you created.
3. Right-click Realms and select Create Realm.
4. In the Agent field, select the Web agent that you created.
5. In the Resource Filter field, enter a protected resource. This resource inherits the protection level specified in the corresponding authentication scheme.
6. For the default protection level, enter /ive-authentication. You must enter this resource when configuring the system. If you use sign-in policies with nondefault URLs such as */nete or */cert, you must have corresponding resource filters in the SiteMinder configuration.

7. From the Authentication Schemes list, select the scheme that you created.
8. Click **OK**.

Configuring a Rule or Response Pair to Pass Usernames

Within SiteMinder, you can use rules to trigger responses during authentication or authorization. A response passes DN attributes, static text, or customized active responses from the SiteMinder policy server to a SiteMinder agent. When you configure SiteMinder to work with the Pulse Secure access management framework, you must create a rule that triggers when a user successfully authenticates. Then, you must create a corresponding response that passes the user's username to the system Web agent.

To create a new rule:

1. Select the Domain tab.
2. Expand the domain that you created and then expand Realms.
3. Right-click the realm that you created and select **Create Rule** under Realm.
4. Enter a name and (optionally) description for the rule.
5. Under Action, select **Authentication Events** and then select **OnAuthAccept** from the drop down list.
6. Select **Enabled**.
7. Click **OK**.

To create a new response:

1. Expand the domain that you created.
2. Right-click Responses and select Create Response.
3. Enter a name and (optionally) a description for the response.
4. Select SiteMinder and then select the Web agent.
5. Click Create.
6. From the Attribute list, select WebAgent-HTTP-Header-Variable.
7. Under Attribute Kind, select Static.

8. Under Variable Name, enter IVEUSERNAME.
9. Under Variable Value, enter a username.
10. Click **OK**.

Configuring Authentication with a SiteMinder Server

To configure authentication with SiteMinder server:

1. Select **Authentication > Auth.Servers**.
2. Select SiteMinder Server and click New Server to display the configuration page.
3. Complete the configuration as described in table.
4. Save the configuration.
5. After you have saved the configuration, the page that is redisplayed includes an Advanced tab.
6. Click the Advanced tab to display the configuration page.
7. Complete the configuration as described in table.
8. Save the configuration.

auth Servers > New SiteMinder Server

New SiteMinder Server

*Name: Label to reference this server

*Policy Server: Name or IP address

Backup Server(s): Comma-delimited list of names or IP addresses

Failover Mode? Yes No

*Agent Name: Name configured on Policy Server

*Secret:

Compatible with: 5.5 Policy Servers

On logout, redirect to: Included for backwards-compatibility. Please use the Custom Pages feature instead.

Protected Resource: /five-authentication Protected resource for authentication as configured on policy server (example: /local-authentication)

Resource Action: GET Resource action for authentication as configured on policy server

Users authenticate using tokens or one-time passwords

[Server Catalog ...](#)

SMSESSION cookie settings

When sending cookies to the end-user's browser:

*Cookie Domain: Example: .company.com

Protocol: HTTPS HTTP Use HTTP to send cookies for all protocols.

When setting cookies on the device:

*Pulse Policy Secure Cookie Domain: Example: .company.com

Protocol: HTTPS HTTP Use HTTPS to send cookies securely.

SiteMinder authentication settings

Automatic Sign In
Check if you want users with a valid SMSESSION cookie to be automatically signed in.
To assign user roles, use this user authentication realm:

If Automatic Sign In fails, redirect to:

Authenticate using custom agent
 Authenticate using HTML form post
 Delegate authentication to a standard agent

[Save Changes](#) [Reset](#)

* Indicates required field

Settings	Guidelines
Name	Specify a name to identify the server within the system.
Policy Server	Specify name or IP address of the policy server.
Backup Server(s)	(Optional) Specify a comma-delimited list of backup policy servers.
Failover Mode?	Select one of the following failover mode options: <ul style="list-style-type: none"> • Yes–The device uses the main policy server unless it fails. • No–The device does the load balancing among all the specified policy servers.
Agent Name	Specify the agent name configured on the policy server.
Secret	Specify the shared secret configured on the policy server. The value is case sensitive.
Compatible with	Select a SiteMinder server version.

Settings	Guidelines
	<ul style="list-style-type: none"> • 5.5 Policy Servers—Supports version 5.5 and version 6.0. This is the default. • 6.0 Policy Servers—Supports only version 6.0 of the SiteMinder server API. • 12.0 Policy Servers—Supports only version 12.0.
On log out, redirect to	Specify a URL to which users are redirected when they sign out of the device (optional). If you leave this field empty, users see the default sign-in page. The On log out, redirect to setting is included in the product release for backwards-compatibility. We strongly recommend that you use the customizable sign-in pages feature instead.
Protected Resource	Specify a default protected resource. If you do not create sign-in policies, the system uses this default URL to set the user's protection level for the session. The system also uses this default URL if you select the Automatic Sign-In option. If your users are signing in to the "*" URL (default device sign-in page), enter any URL ("/ive-authentication" is the default) to set the protection level to the default value. If you do create sign-in policies, the device uses those sign-in policies instead of this default URL. You must enter a forward slash (/) at the beginning of the resource. For example, enter /local-authentication.
Resource Action	Displays the resource action configured on the back-end SiteMinder server.
Users authenticate using tokens or one-time passwords	Select this option if you want the device to prompt the user for a token instead of a password; that is, if users submit tokens or one-time use passwords to the device. For example, you can use this option to dynamically prompt for a password or token based on sign-in policies by configuring two instances of the same authentication server. You can use one instance for wireless users who have this option enabled and it prompts the user for a token, and another instance for wired users who have this option disabled and it prompts the user for a password.
Server Catalog	Use the Server Catalog button to display the Server Catalog in a new window. Add the SiteMinder user attributes (such as the cookienname) that you want to use for role mapping.

Settings	Guidelines
SMSESSION cookie settings	
When sending cookies to the end-user's browser	Specify the cookie domain for either the end user or the device. A cookie domain is a domain in which the user's cookies are active. For example, the system sends cookies to the user's browser in this domain. Multiple domains should use a leading period and be comma-separated. For example, .sales.myorg.com, .marketing.myorg.com. Domain names are case-sensitive. You cannot use wildcard characters
-	Select HTTPS to send cookies securely if other Web agents are set up to accept secure cookies, or HTTP to send cookies non securely.
Cookie Domain and Protocol When the Cookie is Set on the Device	Enter the valid Internet domain for the cookie and where the browser of the user sends cookie contents. This cookie domain should be the same as the host domain. For example, .xyz.net
-	Select HTTPS to send cookies securely if other Web agents are set up to accept secure cookies, or HTTP to send cookies non-securely.
SiteMinder authentication settings	
Automatic Sign In	<p>Select this option to automatically sign in users with a valid SMSESSION cookie. Then, select the authentication realm to which the users are mapped. If you select this option, note that:</p> <ul style="list-style-type: none"> • If the protection level associated with a user's SMSESSION cookie is different from the protection level of the realm, the protection level associated with the cookie is used. • This option uses SMSESSION cookie, which is already present in the browser to enable single sign-on. • This option provides a single sign-on experience for users. • This option enables users to sign in using a standard Siteminder Web Agent that generates an SMSESSION cookie. • When you select this option, you must also configure the following sub options:

Settings	Guidelines
	<ul style="list-style-type: none"> • To assign user roles, use this user authentication realm—Select an authentication realm for automatically signed-in users. The users are mapped to a role based on the role mapping rules defined in the selected realm. • If Automatic Sign In fails, redirect to—Enter an alternative URL for users who sign in through the automatic sign-in mechanism. The users are redirected to the specified URL if the authentication fails and if there is no redirect response from the SiteMinder policy server. If you leave this field empty, users are prompted to sign back in.
Authenticate using custom agent	Select this option if you want to authenticate using the custom Web agent. Using this option, the system generates the SMSESSION cookie, just like any other Web agent configured within the organization.
Authenticate using HTML form post	<p>Select this option if you want to post user credentials to a standard Web agent that you have already configured rather than contacting the SiteMinder policy server directly.</p> <p>If you select this option, the Web agent contacts the policy server to determine the appropriate sign-in page to display to the user.</p> <p>To configure the system to “act like a browser” that posts credentials to the standard Web agent, you must enter the following information.</p> <ul style="list-style-type: none"> • Target—Specify the target URL. • Protocol—Specify the protocol for communication between the system and the specified Web agent. Select HTTP for non-secure communication. Select HTTPS for secure communication. <p>• Webagent—Specify the name of the Web agent to obtain SMSESSION cookies. An IP address is not allowed for this field. (Specifying the IP address as the Web agent prevents some browsers from accepting cookies.)</p> <ul style="list-style-type: none"> • Port— Specify the port for the protocol. Enter port 80 for HTTP or port 443 for HTTPS. • Path—Specify the path of the Web agent’s sign-in page. The path must start with a backslash (/) character. In the Web agent sign-in page URL, the path appears after the Web agent.

Settings	Guidelines
	<ul style="list-style-type: none"> Parameters– Specify the post parameters to be sent when a user signs in. Common SiteMinder variables that you can use include <code>__USER__</code>, <code>__PASS__</code>, and <code>__TARGET__</code>. These variables are replaced by the username and password entered by the user on the Web agent's sign-in page and by the value specified in the Target field. These are the default parameters for log in.fcc—if you have made customizations, you may need to change these parameters.
Delegate authentication to a standard agent	<p>Select this option to delegate authentication to a standard agent. When the user accesses the system sign-in page, the FCC URL associated with the protected resource's authentication scheme is determined. The system redirects the user to that URL, setting the system sign-in URL as the target. After successfully authenticating with the standard agent, an SMSESSION cookie is set in the user's browser and the user is redirected back. The system then automatically signs in the user and establishes a session.</p> <p>You must enable the Automatic Sign-In option to use this feature. If you enable this option and a user already has a valid SMSESSION cookie when trying to access a resource, the system tries to automatically sign in using the existing SMSESSION cookie. If the cookie is invalid, the SMSESSION cookie and corresponding system cookies are cleared and a "timeout" page is displayed. The system successfully delegates authentication when the user clicks the sign back in option. If you select this option, your authentication scheme must have an associated FCC URL.</p>

Settings	Guidelines
Poll Interval (seconds)	Specify the interval at which the system polls the SiteMinder policy server to check for a new key.
Max. Connections	Control the maximum number of simultaneous connections that the system is allowed to make to the policy server. The default setting is 20.
Max. Requests/Agent	Control the maximum number of requests that the policy server connection handles before the system ends the connection. If necessary, tune to increase performance. The default setting is 1000.

Settings	Guidelines
Idle Timeout (minutes)	Control the maximum number of minutes a connection to the policy server may remain idle (the connection is not handling requests) before the system ends the connection. The default setting of "none" indicates no time limit.
Authorize while Authenticating	Specify that the system should look up user attributes on the policy server immediately after authentication to determine if the user is truly authenticated. For example, if your SiteMinder server authenticates users based on an LDAP server setting, you can select this option to indicate that the system should authenticate users through the SiteMinder server and then authorize them through the LDAP server before granting them access. If the user fails authentication or authorization, the user is redirected to the page configured on the policy server.
Enable Session Grace Period	Eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the system should consider the cookie valid for a certain period. If you do not select this option, the system checks the user's SMSESSION cookie on each request. Note that the value entered here does not affect session or idle timeout checking.
Validate cookie every N seconds (seconds)	Specify the time for the system to eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the system should consider the cookie valid for a certain period.
Ignore Query Data	Specify that the system does not cache the query parameter in its URLs. Therefore, if a user requests the same resource as is specified in the cached URL, the request should not fail.
Accounting Port	Specify that the value entered in this field must match the accounting port value entered through the Policy Server Management Console in the Web UI. By default, this field matches the policy server's default setting of 44441.
Authentication Port	Specify that the value entered in this field must match the authentication port value entered through the Policy Server Management Console. By default, this field matches the policy server's default setting of 44442.
Authorization Port	Specifies that the value entered in this field must match the authorization port value entered through the Policy Server Management Console. By default, this field matches the policy server's default setting of 44443.
Agent Configuration Settings	

Settings	Guidelines
Overlook Session for Methods	<p>Compare the request method to the methods listed in this parameter. If a match is found, Web Agent does not create a new or update an existing SMSESSION cookie, nor will it make any updates to the cookie provider for that request.</p> <p>You can enter multiple methods; use a comma to separate method names.</p> <p>If Overlook Session for Methods parameter is set but not Overlook Session for URLs, then all requests that match the methods defined in this parameter are processed (SMSESSION cookie creation/update is blocked).</p> <p>If both Overlook Session for Methods and Overlook Session for URLs parameters are set, both the method and the URL of the request are matched before proceeding. Then, all URLs with specified methods are processed (SMSESSION cookie creation/update is blocked).</p>
Overlook Session for URLs	<p>Compare the request URL to the URLs listed in this parameter. If a match is found, Web Agent does not create a new or update an existing SMSESSION cookie, nor will it make any updates to the cookie provider for that request.</p> <p>Specify a relative URL. For example: If the URL is <code>http://fqdn.host/MyDocuments/index.html</code>, enter <code>/MyDocuments/index.html</code></p> <p>If Overlook Session for URLs is set but not Overlook Session for Methods, then all requests, regardless of the methods, matching the URLs defined in this parameter are processed (SMSESSION cookie creation/update is blocked).</p> <p>If both Overlook Session for Methods and Overlook Session for URLs parameters are defined, both the method and the URL of the request are matched before proceeding. Then, all URLs with specified methods are processed (SMSESSION cookie creation/update is blocked).</p>
SiteMinder caching	
Flush Cache	Select this option to delete the resource cache, which caches resource authorization information for 10 minutes.

Displaying the User Accounts Table

To display user accounts:

1. Click the link for the authentication server you want to manage.
2. Click the **Users** tab to display the user accounts table.

The user accounts table includes entries for the accounts that have been created. The Last Sign-in Statistic column shows the last successful sign-in date and time for each user, the user's IP address, and the agent or browser type and version.

Use the controls to search for users and manage user accounts:

- To search for a specific user, enter a username in the Show users named box and click Update.



You can use an asterisk (*) as a wildcard, where * represents any number of zero or more characters. For example, to search for all usernames that contain the letters jo, enter *jo*. The search is case-sensitive. To display the entire list of accounts again, type * or delete the field's contents and click Update.

- To limit the number of users displayed on the page, enter a number in the Show N users box and click Update.
- To terminate the user session and delete the account, select the check box next to the user account record and click **Delete**.

Troubleshooting the SiteMinder Server Configuration

Problem	Description: At some point, you may encounter problems configuring the eTrust SiteMinder server interactions with the Ivanti system. You can use the following debugging tools to identify and resolve problems:
---------	--

Solution

- Review the system log file. The system tracks failures of cookie validation and key rollovers.
- Review the Policy Server Authentication log files.
- Review the Standard Web Agent log file if you selected the Authenticate using HTML Form POST option.
- Confirm that the system time is synchronized with the SiteMinder server system time. If the two system times are too divergent, the timeout settings might not function correctly, and might reject attempts to sign in.

- In the SiteMinder server, confirm that you have defined the proper Session Timeout options max timeout and idle in the SiteMinder Realm dialog.
- To view the CA SiteMinder error codes select **System > Log/Monitoring > User Access** page. For information on the CA SiteMinder error codes, see the SiteMinder documentation.

Using an SQL Auth Server

This topic describes integration with the SQL Auth server.

SQL Auth Server Overview

This section describes support for using the SQL (also known as Oracle Database server) as a IPS authentication server. It includes the following sections:

Understanding SQL Auth Server

The SQL Auth server is widely deployed in the enterprise. Some enterprises use the SQL Auth server to store user credentials (usernames and passwords), MAC addresses, and other organizational information, such as group affiliations that are often the basis for authorization decisions. To support authentication and authorization against SQL Auth server databases, IPS supports an authentication server configuration that configures an Oracle Instant Client connection as well as relevant queries to the backend SQL Auth server.

Feature Support

Policy Secure uses Oracle Instant Client 11.2.0.2.0 to communicate with the SQL Auth server. The SQL Auth server version must support this version of the client. The Pulse Secure access management framework depends on the SQL Auth server features described in this section.

You can use the SQL queries for authentication, authorization and role mapping, or both.

SQL SELECT Statements

The authentication transaction is based on an SQL query that returns a password (and possibly other information) based on the name entered by the user attempting to log in.

While a sample SQL query is provided in the original configuration file, you must configure the SQL entry of the configuration file with a query appropriate to your database. The query you enter must be either an SQL SELECT or an SQL EXECUTE statement that contains additional syntax elements that are preprocessed by the SQL authentication module.

The SQL authentication module executes SQL statements in parameterized form. This means that the SQL statement is compiled once, with parameter markers (usually question marks) as placeholders for data items that vary from one execution to the next. Only upon execution of the statement are the actual data values supplied.

The SQL statement you compose must not include parameter markers directly. Instead, include the names of the parameters where parameter markers would appear, in an appropriate format.

This is an example of a parameter marker:

1. SELECT password, profile, fullname FROM usertable WHERE username = :username
2. The SQL authentication module translates the SQL statement provided, replacing parameter names with parameter markers prior to passing the SQL statement to the database engine.
3. The SQL statement can be very simple. Basically, all that is required is to look up a password and possibly some optional information based on a username. The SQL statement can also be quite complex; it can include inner joins, and it can contain expressions. The underlying database engine is responsible for handling the SQL statement; the SQL authentication module performs no interpretation of the SQL statement other than to translate parameter names to parameter markers.

SQL Stored Procedures

A stored procedure is a sequence of SQL statements that form a logical unit and perform a task. You can use stored procedures to encapsulate a set of queries or operations that can be executed repeatedly on a database server. For example, you can code operations on an employee database, such as password lookup, as stored procedures that can be executed by application code. Stored procedures can be compiled and executed with different parameters and results. Stored procedures can use any combination of input parameters (the values passed to the stored procedure at execution time) and output parameters (the values set or returned by the stored procedure to the calling application or environment).

Vendor	Example of a called procedure
Oracle	BEGIN; myCalledProcedure(:username, :password!os, ipAddr!ios, filterId!o); END;

MySQL	CALL myCalledProcedure(:username, :password!os, ipAddr!ios, filterId!o);
MSSQL	{CALL myCalledProcedure(:username, :password!os, ipAddr!ios, filterId!o)}

As shown in the example, the procedure is called `myCalledProcedure` with input variables as `username` and `ipAddr`, output parameters as `password`, `ipAddr`, and `filterId`. The names of the output parameters are the names of the attributes added to the server catalog used for role mapping and return attributes. The parameter consists of a colon (:), the name of the parameter, and a format specifier.

SQL Format Specifiers

Table describes the SQL statement format specifiers with parameters in called procedures.

Specifier	Definition
i	Input parameter (Default if none is specified)
io	Input/output parameter
o	Output parameter
s	String type (default if none is specified)
n	Int type

SQL Statement Parameters

Table describes the SQL statement parameter names and types.

Item	Type	Meaning for SQL Authentication
:username	String	Specifies the username as presented to the authentication server.
:password	String	Specifies the password as presented to the authentication server.
:realm	String	Specifies the realm as presented to the authentication server.
:ipAddr	String	Specifies the source IP address (L3 authentications only), which is sent as a string. For example, 10.17.1.155.
:userAgent	String	Specifies the user agent string.
:log inTime	Int	Specifies the log in time presented in the number of seconds.

Item	Type	Meaning for SQL Authentication
:log inURL	String	Specifies the user URL of the sign-in policy of the user.
:callingStationId	String	Specifies the MAC address of the client presented as xx-xx-xx-xx-xx-xx for L3 authentications and in the format specified by the RADIUS client for L2 authentications.
:language	String	Specifies the language used by client as specified by IETF language tag. For example, en-US for English as used in the United States.

SQL Password Hash Format

Table describes the different SQL password types.

Hash/Name	Definition	Password Format	Supported RADIUS Protocols
Automatic	Automatically determines hash format based on Format.	All	
Clear Text	No Encryption	PasswordText	PAP, CHAP, MSCHAP, MSCHAP-V2, EAP-JUAC, EAP-MSCHAP-V2, EAP-MD5-Challenge
SHA 1	SHA1+Base64 hash	{SHA}HashHashHash	PAP, EAP-JUAC
Salted SHA 1	salted SHA1+Base64 hash	{SSHA}HashHashHashSalt	PAP, EAP-JUAC
NT Hash**	MD4 hash of the unicode form of password	{md4}HashHash	PAP, MSCHAP, MSCHAP-V2, EAP-JUAC, EAP-MSCHAP-V2

Interoperability Requirements and Limitations

The following limitation applies when defining and monitoring an SQL Auth server instance:

- The maximum number of connections to an Oracle database is limited to 50 connections for L2 and L3 log ins (concurrent and open RADIUS protocol), without any browser log ins.
- You must enter the SQL keywords in uppercase letters.

Configuring Authentication with an Oracle SQL Auth Server

To configure authentication with an SQL Auth server:

1. Select **Authentication > Auth.servers**.
2. Select SQL Auth Server and click New Server to display the configuration page.
3. Select the SQL Vendor as Oracle. Complete the configuration as described in
4. Save the configuration.

Auth Servers > oracle > Settings

Settings

Settings | Users

*Name: Label to reference this server.

*SQL Vendor:

*SQL Auth Server: Name or IP address

*SQL Port:

Backup SQL Auth Server: Name or IP address

Backup SQL Port:

SQL Service Name: SQL Service/Database Name

*Admin:

*Password:

*Connection Timeout: Seconds to wait for connection to SQL Auth server (Min 5, Max 120)

*Search Timeout: Seconds to wait for search results, excluding connection time (Min 5, Max 120)

*You have Agreed to the Oracle Instant Client License Agreement

▼ Finding user entries

*SQL Statement: example: SELECT password FROM usertable WHERE username = :username AND realm = :realm

Password Attribute Name: attribute from SELECT list that contains password

Full Username Attribute Name: attribute from SELECT list that contains Full User Name

SQL Password Type:

▼ Test User Lookup


Select Statement Values:

Save SQL Column Names or Called Procedure variable names as Attribute names in the Server Catalog

Results:

▼ Server Catalog

* indicates required field

Settings	Guidelines
Name	Specify a name to identify the server within the system.
SQL Vendor	Select Oracle. Read and accept the license agreement. You cannot save or test the configuration until you have accepted the license agreement.
SQL Auth Server	Specify the SQL Auth server host name or IP address. The default value is 1521.
SQL Port	Specify the SQL port number through which the SQL Auth server is accessed.
Backup SQL Auth Server	(Optional) Specify the backup SQL Auth server host name.
Backup SQL Port	(Optional) Specify the backup SQL port number.
SQL Service Name	(Optional) Specify the SQL service name if SQL service name has been defined in the SQL Auth server configuration.
Admin	Specify the administrator username.
Password	Specify the password.
Connection Timeout	Specify the connection timeout value from 5 to 60 seconds. If this time is exceeded, and if there is a backup server defined, then the device attempts to reach the backup server.
Search Timeout	Specify the search timeout value from 5 to 60 seconds. It specifies the maximum amount of time the device will wait for the SQL Auth server to return search results.
Finding user entries	
SQL Statement	<p>Specify the SQL statement to find the user entries.</p> <p>For example:</p> <pre>SELECT password FROM usertable WHERE username = :username AND realm = :realm</pre> <hr/> <p> You must enter the SQL keywords in uppercase letters.</p> <hr/>

Settings	Guidelines
Password Attribute Name	Specify the attribute name specified in the SQL statement that the device uses for password authentication. If the username that is entered exists in the database, then the authentication succeeds. If you are using the SQL Auth server for authorization, no password is necessary here.
Full Username Attribute Name	(Optional) Specify the attribute name specified in the SQL statement for the system to use when displaying the user's full name.
SQL Password Type	<p>Select one of the following SQL password types:</p> <ul style="list-style-type: none"> • Automatic • Clear Text • SHA 1 • Salted SHA 1 • NT Hash <p>The SQL password type setting specifies the format of the hash used for the password. The values for the SQL password type include a prefix index that indicates how the password has been processed. The prefix is in clear-text between curly braces { } and is immediately followed by a hash value computed from the password. If no prefix is present in the value retrieved from the table Password column, the entire password is assumed to be in clear-text format.</p>
Test User Lookup	
Select Statement Values	Enter the attributes necessary to fill in the WHERE part of the SQL statement and click the Test Connection button to save the server configuration and attempt to connect to the database server with the information you have entered
Save SQL Column Names or Called Procedure variable names as Attribute names in the Server Catalog	Select this option to use the SQL query statement variables as server catalog attributes. You can use the server catalog in role mapping rules.

Settings	Guidelines
Server Catalog	
Attributes	The Attributes button appears after you have saved the server information or performed a test connection operation. Click the Attributes button to display the server catalog.

Configuring Authentication with MySQL Auth Server

To configure authentication with an SQL Auth server:

1. Select **Authentication > Auth.servers**.
2. Select **SQL Auth Server** and click **New Server** to display the configuration page.
3. Select the SQL vendor as MYSQL.
4. Complete the configuration as described in table
5. Save the configuration.

Auth Servers > MySQL > Settings

Settings

Settings Users

*Name: Label to reference this server.

*SQL Vendor:

*SQL Auth Server: Name or IP address

*SQL Port:

Backup SQL Auth Server: Name or IP address

Backup SQL Port:

SQL Service Name: SQL Service/Database Name

*Admin:

*Password:

*Connection Timeout: Seconds to wait for connection to SQL Auth server(Min 5, Max 120)

*Search Timeout: Seconds to wait for search results, excluding connection time(Min 5, M

Use SSL:

Server Certificate Validation:

▼ Finding user entries

*SQL Statement: example: SELECT password FROM usertable WHERE usern

Password Attribute Name: attribute from SELECT list that contains password

Full Username Attribute Name: attribute from SELECT list that contains Full User Name

SQL Password Type:

▼ Test User Lookup

Select Statement Values:

Save SQL Column Names or Called Procedure variable names as Attribute names in the Server Catalog


Results:

▼ Server Catalog

* indicates required field

Settings	Guidelines
Name	Specify a name to identify the server within the system.
SQL Vendor	Select MYSQL as the vendor type.
SQL Auth Server	Specify the SQL Auth server host name or IP address. The default value is 1521.
SQL Port	Specify the SQL port number through which the MYSQL Auth server is accessed. Default port is 3306.
Backup SQL Auth Server	(Optional) Specify the backup SQL Auth server host name.
Backup SQL Port	(Optional) Specify the backup SQL port number.
SQL Service Name	(Optional) Specify the SQL service name if SQL service name has been defined in the SQL Auth server configuration.
Admin	Specify the administrator username.
Password	Specify the password.
Connection Timeout	Specify the connection timeout value from 5 to 60 seconds. If this time is exceeded, and if there is a backup server defined, then the device attempts to reach the backup server.
Search Timeout	Specify the search timeout value from 5 to 60 seconds. It specifies the maximum amount of time the device will wait for the SQL Auth server to return search results.
Use SSL	Select Use SSL to establish an encrypted connection between the client and server.
Server Certificate Validation	Select this option to validate the server certificate before using the public and private keys for encryption/decryption.
Finding user entries	
SQL Statement	Specify the SQL statement to find the user entries.
Password Attribute Name	Specify the attribute name specified in the SQL statement that the device uses for password authentication. If the username that is entered exists in the database, then the authentication succeeds. If you are using the SQL Auth server for authorization, no password is necessary here.

Settings	Guidelines
Full Username Attribute Name	(Optional) Specify the attribute name specified in the SQL statement for the system to use when displaying the user's full name.
SQL Password Type	<p>Select one of the following SQL password types:</p> <ul style="list-style-type: none"> • Automatic • Clear Text • SHA 1 • Salted SHA 1 • NT Hash <p>The SQL password type setting specifies the format of the hash used for the password. The values for the SQL password type include a prefix index that indicates how the password has been processed. The prefix is in clear-text between curly braces { } and is immediately followed by a hash value computed from the password. If no prefix is present in the value retrieved from the table Password column, the entire password is assumed to be in clear-text format.</p>
Test User Lookup	
Select Statement Values	<p>Enter the attributes necessary to fill in the WHERE part of the SQL statement and click the Test Connection button to save the server configuration and attempt to connect to the database server with the information you have entered.</p> <p>Upon a successful connection and retrieval of the user record, the server displays the results. It displays the entire returned user record (hiding the password) from the SELECT portion of the SQL statement. An error line is displayed if the connection to the SQL Auth server fails or if the user record could not be retrieved. The user record is displayed in the following format: attribute Name1 = value, attribute name2 = value, and so on.</p>


Settings	Guidelines
	<p> When trying to populate the server catalog attributes for the SQL Auth server, you must enter data into all columns of interest for a record. Columns that are not assigned data are ignored during the lookup and are therefore not added appropriately to the server catalog.</p>
Save SQL Column Names or Called Procedure variable names as Attribute names in the Server Catalog	Select this option to use the SQL query statement variables as server catalog attributes. You can use the server catalog in role mapping rules.
Server Catalog	
Attributes	The Attributes button appears after you have saved the server information or performed a test connection operation. Click the Attributes button to display the server catalog.


Configuring Authentication with MSSQL Auth Server

To configure authentication with an SQL Auth server:

1. Select **Authentication > Auth.servers**.
2. Select **SQL Auth Server** and click **New Server** to display the configuration page.
3. Select the SQL vendor as MSSQL.
4. Complete the configuration as described in table
5. Save the configuration.

Settings	Guidelines
Name	Specify a name to identify the server within the system.
SQL Vendor	Select MSSQL as the vendor type.
SQL Auth Server	Specify the MSSQL Auth server host name or IP address.

Settings	Guidelines
SQL Port	Specify the MSSQL port number through which the MYSQL Auth server is accessed. Default port is 1433.
Backup SQL Auth Server	(Optional) Specify the backup MSSQL Auth server host name.
Backup SQL Port	(Optional) Specify the backup MSSQL port number.
SQL Service Name	(Optional) Specify the SQL service name if SQL service name has been defined in the SQL Auth server configuration.
Admin	Specify the administrator username.
Password	Specify the password.
Connection Timeout	Specify the connection timeout value from 5 to 60 seconds. If this time is exceeded, and if there is a backup server defined, then the device attempts to reach the backup server.
Search Timeout	Specify the search timeout value from 5 to 60 seconds. It specifies the maximum amount of time the device will wait for the SQL Auth server to return search results.
Use SSL	Select Use SSL to establish an encrypted connection between the client and server.
Server Certificate Validation	<p>Select this option to validate the server certificate before using the public and private keys for encryption/decryption.</p> <hr/> <p> The server certificate validation for MSSQL is qualified using self signed certificate.</p> <hr/>
Finding user entries	
SQL Statement	Specify the SQL statement to find the user entries.
Password Attribute Name	Specify the attribute name specified in the SQL statement that the device uses for password authentication. If the username that is entered exists in the database, then the authentication succeeds. If you are using the SQL Auth server for authorization, no password is necessary here.
Full Username Attribute Name	(Optional) Specify the attribute name specified in the SQL statement for the system to use when displaying the user's full name.

Settings	Guidelines
SQL Password Type	<p>Select one of the following SQL password types:</p> <ul style="list-style-type: none"> • Automatic • Clear Text • SHA 1 • Salted SHA 1 • NT Hash <p>The SQL password type setting specifies the format of the hash used for the password. The values for the SQL password type include a prefix index that indicates how the password has been processed. The prefix is in clear-text between curly braces { } and is immediately followed by a hash value computed from the password. If no prefix is present in the value retrieved from the table Password column, the entire password is assumed to be in clear-text format.</p>
Test User Lookup	
Select Statement Values	<p>Enter the attributes necessary to fill in the WHERE part of the SQL statement and click the Test Connection button to save the server configuration and attempt to connect to the database server with the information you have entered.</p> <p>Upon a successful connection and retrieval of the user record, the server displays the results. It displays the entire returned user record (hiding the password) from the SELECT portion of the SQL statement. An error line is displayed if the connection to the SQL Auth server fails or if the user record could not be retrieved. The user record is displayed in the following format: <u>attribute Name1 = value, attribute name2 = value, and so on.</u></p> <p> When trying to populate the server catalog attributes for the SQL Auth server, you must enter data into all columns of interest for a record. Columns that are not assigned data are ignored during the lookup and are therefore not added appropriately to the server catalog.</p>

Settings	Guidelines
Save SQL Column Names or Called Procedure variable names as Attribute names in the Server Catalog	Select this option to use the SQL query statement variables as server catalog attributes. You can use the server catalog in role mapping rules.
Server Catalog	
Attributes	The Attributes button appears after you have saved the server information or performed a test connection operation. Click the Attributes button to display the server catalog.

Troubleshooting Oracle Error Codes

Table describes the Oracle error codes, cause, and action.

Error code	Cause	Action
ORA-00018: maximum number of sessions exceeded	All session state objects are in use.	Increase the value of the SESSIONS initialization parameter.
ORA-00019: maximum number of session licenses exceeded	All licenses are in use.	Increase the value of the LICENSE MAX SESSIONS initialization parameter.
ORA-00020: maximum number of processes (string) exceeded	All process state objects are in use.	Increase the value of the PROCESSES initialization parameter.

Using a Time-Based One-Time Password (TOTP) Authentication Server

This topic describes IPS integration with the Time-Based One-Time Password (TOTP) Authentication

Overview

This section describes support for using the Local/Remote IPS TOTP authentication server.

Understanding TOTP

Time-based One-time Password Algorithm (TOTP) is an algorithm that computes a one-time password (token) from a shared secret key and the current time. Google Authenticator is one of such implementations of TOTP algorithms. IPS supports TOTP authentication by using the Google Authenticator algorithm for generation of shared secret key and token. Many third-party aIPS are available for almost all mobile and desktop operating systems for the generation of TOTP tokens.

Interoperability Requirements and Limitations

Before you begin:

TOTP authentication server users' configuration is automatically synchronized within all nodes in a single cluster. If there are multiple clusters behind a DNS load-balancer, then the admin has to manually perform binary export/import user's configuration to all the nodes in different clusters.

TOTP feature is configurable across clusters.

First time users have to register a new TOTP user-account via web. End-users cannot use Pulse Desktop applications and Pulse Mac applications for new user registration.

CAUTION: Users with more than one TOTP account will be reset when the system software is upgraded. In such case, users have to re-register with TOTP.

Two standalone nodes or separate clusters can be synced. For now, binary import/export of user configuration option can be used.



For the users who are already using custom sign-in pages:

For TOTP authentication to work, existing custom sign-in pages need to include following sign-in pages:

- `TotpAuthRegister.shtml`
- `TotpAuthRegister-mobile-webkit.shtml`
- `TotpAuthRegister-ipad.shtml`
- `TotpAuthRegister-stdaln.shtml`
- `TotpAuthRegister-new-ux.shtml`
- `TotpAuthTokenEntry.shtml`

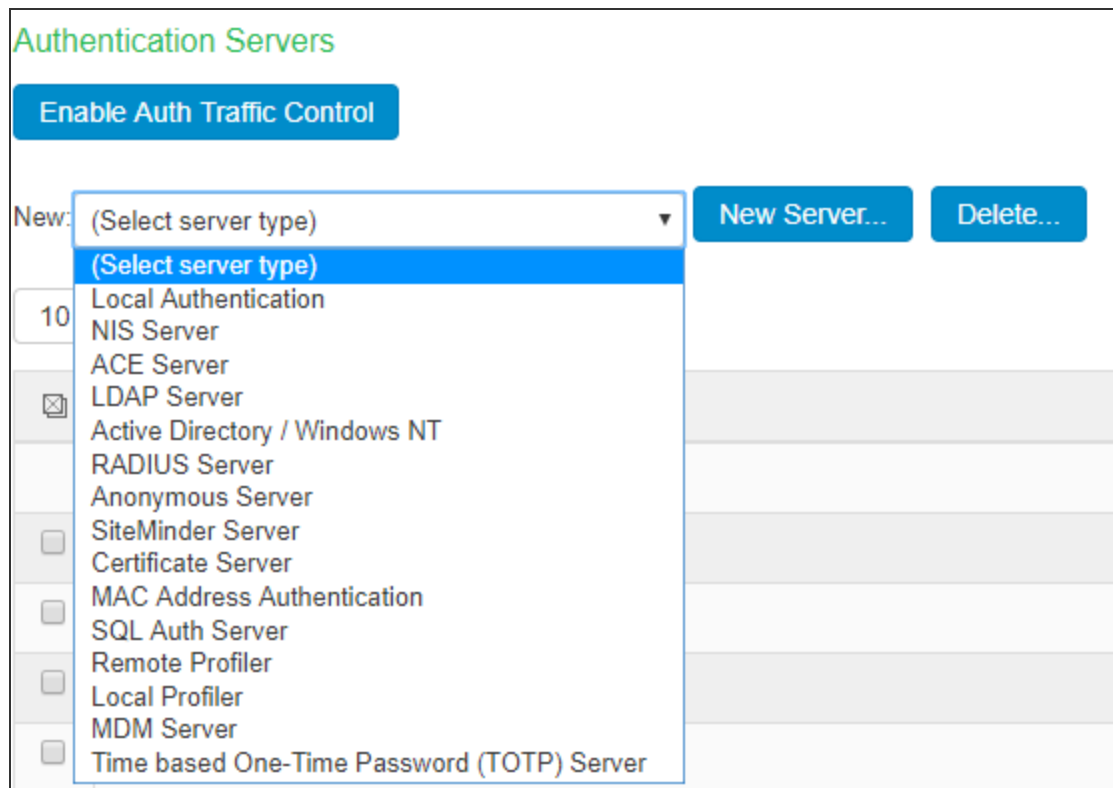
- TotpAuthTokenEntry-new-ux.shtml
- TotpAuthTokenEntry-mobile-webkit.shtml
- TotpAuthTokenEntry-ipad.shtml
- TotpAuthTokenEntry-stdaln.shtml

These files can be downloaded from sample custom sign-in pages URL: <https://<IPS>/dana-admin/download/sample.zip?url=/dana-admin/auth/custompage.cgi?op=Download&samplePage=sample>

Configuring Authentication with a TOTP Authentication Server

To configure the TOTP server as Local:

1. Select **Authentication > Auth. Servers**.
2. Select **Time based One-Time Password (TOTP)** Server and click **New Server** to display the configuration page.



3. Complete the configuration as described in table.

4. Save the configuration.

The screenshot shows the configuration page for a TOTP server. The breadcrumb is 'Auth Servers > TOTP_Local > Settings'. The page has two tabs: 'Settings' (active) and 'Users'. The configuration fields are as follows:

- Name:** TOTP_Local (Label to reference this server)
- Server Type:** Local (selected), Remote
- Time Skew:** 5 minutes (Max time difference between pulse secure appliance and end user device while authenticating a user's token)
- Number of attempts allowed:** 4 (Max number of consecutive wrong attempts allowed after which account will be locked)
- Custom message for registration page:** (Empty text area)
- Allow Auto Unlock:** (Checked checkbox)
- Allow new TOTP user registration to happen via external port:** (Unchecked checkbox)
- Accept TOTP authentication from remote Pulse Secure devices:** (Checked checkbox)
- Display QR code during user registration:** (Checked checkbox)
- Disable generation of backup codes:** (Checked checkbox)

Buttons at the bottom: 'Save Changes' and 'Reset'. A note at the bottom left states '* indicates required field'.

Settings	Guidelines
Name	Specify a name to identify the server within the system.
Server Type	TOTP server can be configured as local or remote. Select Local. Local: TOTP context is created locally and user database is maintained locally on the same device.
Time Skew	Specify maximum time difference between IPS and end user device while authenticating a user's token. (minimum: 1 minute, maximum: 5 minutes).
Number of attempts allowed	Specify maximum number of consecutive wrong attempts allowed after which account will be locked (minimum: 1 attempt, maximum: 5 attempts).
Custom message for registration page	Specify a custom message which can be shown on new TOTP user registration web-page.
Allow Auto Unlock	When checked, locked account will be automatically unlocked after specified period. (minimum: 10 minutes, maximum: 90 days)
Allow new TOTP user registration to happen via external port	When unchecked (default), new TOTP user registrations will happen only via internal port

Settings	Guidelines
Accept TOTP authentication from remote internal devices	When checked, REST access to this TOTP server is allowed from other internal devices.
Display QR code during user registration	When checked, displays QR code during user registration.
Disable generation of backup codes	When unchecked, generates backup codes.

To configure the TOTP server as Remote:

1. Select **Authentication > Auth. Servers**.
2. Select Time based One-Time Password (TOTP) Server and click New Server to display the configuration page. See figure
3. Complete the configuration as described in table.
4. Save the configuration.



If IPS is configured to use Remote TOTP server, then the remote server should have a valid certificate issued by a Trusted CA.

Auth Servers > TOTP Remote > Settings

Settings

Settings Users

*Name: Label to reference this server.

Server Type: Local Remote

Allow new TOTP user registration to happen via external port When unchecked (default), new TOTP user registrations will happen only via company intranet network

*Host Name/IP: Remote hostname or IP where TOTP server is configured.

*TOTP Server Name: TOTP server name on remote host.

*REST API Login: REST API login name.

*REST API Password: REST API password.

*REST Authentication Realm: Realm to be used for REST Authentication

Check server reachability without saving your changes

* indicates required field

Settings	Guidelines
Name	Specify a name to identify the server within the system.

Settings	Guidelines
Server Type	TOTP server can be configured as local or remote. Select Remote. Remote: In this configuration, authentication check happens on the remote TOTP server. The user local device acts as a proxy between the user's client device and TOTP server. The communication to the remote device happens on REST API.
Allow new TOTP user registration via external port	Enable this option to allow TOTP user registrations through external port.
Host Name/IP	Specify remote host name or IP address where the TOTP server is configured.
TOTP Server Name	This is the name of the TOTP server configured on the Remote TOTP server.
REST API Login	Enter the REST API login name.
REST API Password	Enter the REST API password.
REST Authentication Realm	Enter the realm name, which refers to the realm that should be used for authenticating the rest user (using the authserver mapped to the Realm).

Configuring Admin/User Realm to Associate a TOTP Authentication Server as Secondary Authentication Server

For example, to configure a user realm:

1. Select **Users > User Realms > New User Realm**.
2. Complete the settings for the user-realm.
3. Check the Enable additional authentication server option.

- Under Additional Authentication Server, select any already created TOTP authentication-server from the Authentication #2 dropdown, as shown in table.



Whenever admin selects TOTP authentication-server as the additional authentication server, then the Username: Predefined as <USER> and Password: specified by user in sign-in page options are set by default.

- Click on **Save Changes**.

The screenshot shows the 'General' tab of the 'Users' realm configuration. The 'Name' is 'Users' and the 'Description' is 'Default authentication realm for users'. Under the 'Servers' section, the 'Authentication' is set to 'AD_200.100', 'User Directory/Attribute' is 'Same as above', 'Accounting' is 'None', and 'Device Attributes' is 'None'. In the 'Additional Authentication Server' section, 'Enable additional authentication server' is checked. Under 'Authentication #2', 'TOTP_Server' is selected. The 'Username is' dropdown is set to 'predefined as <USER>' and the 'Password is' dropdown is set to 'specified by user on sign-in page'. The 'End session if authentication against this server fails' checkbox is also checked.

Using [Google Authenticator](#) Application to Register to a TOTP Server


The admin can associate an end-user to a realm that has a secondary authentication server configured as TOTP authentication server.

For first time registration via web, perform the following steps:

For example: Admin associates an end-user User1 to a user-realm that has the TOTP authentication-server configured as the secondary authentication-server.

When User1 for the first time, performs a login to the above configured user-realm:

1. After successful authentication with primary authentication-server, User1 is shown the TOTP registration page. See figure
2. User1 is given a TOTP registration key in text form/QR image form and 10 backup codes. User saves 10 backup codes in a safe place for using it later during authentication when end-user device (where Google Authenticator app is installed) is not available (in emergency).
3. Now, User1 opens the device where Google Authenticator app is installed, then either scans the QR image (or) manually adds a new user (for example: GA-User1) by entering the above given secret registration key.
4. The Google-Authentication app (for GA-User1) generates a new 6-digit number called as a token once in every 30 seconds.
5. Enter the current token in the registration page. Click on **Sign In**. On successful authentication with that token, User1 will be taken to his/her home page.

 Pulse Secure

Welcome to Pulse Policy Secure


Add *totp-user* user account to your two factor authentication app

You will need to install a two factor authentication application (Google Authenticator) on your smartphone or tablet.

1. Configure the App:

Open your two factor authentication app and add "totp-user" user account by scanning the below QR code.

If you can't use QR code, then enter [this text](#).



2. Store Backup Codes:

Backup codes can be used to access your account in the event you lose access to your device and cannot receive two-factor authentication codes. Following backup codes are only for one time use, we recommend you to save them securely.

ZHQC4H	2WQM6O
FKTTYW	3WHCS5
KJRO3O	B5VGX7
JB4WSO	SPYGVO
2QEFIH	OJJEY4

3. Enter token code that the application generates:

For already registered user, perform the following steps:

1. The already-registered user (For example: User1), whose realm was associated with secondary authentication server configured as TOTP authentication server, accesses IPS URL via web (User1 has already registered TOTP user in Google Authenticator app.)
2. After successful authentication with primary authentication server, user1 is shown TOTP Token entry page as seen in figure
3. User1 opens Google Authentication app that was installed in mobile (or PC), enters the current token to the

4. Authentication Code. If mobile is not available, user can enter any of the unused backup codes.
5. On successful authentication with the token, User1 can enter any of the unused backup codes.



A backup code can be used only once to successfully authenticate with the TOTP authentication server. Once used, the same backup code cannot be reused.

Welcome to
Ivanti Policy Secure

Two-Factor Authentication for *totp-user*

Open the two-factor authentication app on your device to view your authentication code and verify your identity .

Currently if you do not have access to your device, use one of the backup codes saved previously.

Authentication code:

Displaying the User Accounts Table

To display user accounts:

1. Select **Authentication > Auth.Servers**.
2. Click the link for the authentication server you want to manage.
3. Click the Users tab to display the user accounts table. The Last Sign-in Statistic column shows the last successful sign-in date and time for each user, the user's IP address, and the agent or browser type and version.
 - The "Last Attempted" column shows the last time and date a user attempted to login.
 - The "Last Successful Login" shows the last successful sign-in date and time for each user.
4. Under the "User Information" column, there are details available for a user's "Realm", "Primary AuthServer" and the "Status" columns.

There are 3 possible states for the "Status" column:

- Active: TOTP user's account is in use (that is user has used this account less than stale period of this TOTP authentication server)
- Locked: TOTP user account has been locked due to maximum number of wrong login attempts

- Unregistered: TOTP user has seen registration page, but yet to complete the registration by entering the correct token in the registration page.

Use the controls to search for users and manage user accounts:

To search for a specific user, enter a username in the Show users named field and click Update.



You can use an asterisk (*) as a wildcard, where * represents any number of zero or more characters. For example, to search for all usernames that contain the letters jo, enter *jo*. The search is case-sensitive. To display the entire list of accounts again, type * or delete the field's contents and click Update.

To limit the number of users displayed on the page, enter a number in the Show N user's field and click Update.

To unlock a user, select the specific user and click **Unlock**.

To reset a user's credentials, select the specific user and click **Reset**.

	Username	Last Attempted	Last Successful Login	User Information		
				Realm Registered From	Realm Last Logged In	Status
<input type="checkbox"/>	annef	2019/02/27 11:10:56	2019/02/27 11:10:56	Users	Users	Active
<input type="checkbox"/>	unregistered	2019/02/27 11:11:18		Users		Unregistered
<input type="checkbox"/>	emma	2019/02/27 11:16:36	2019/02/27 11:16:36	Users	Users	Active
<input type="checkbox"/>	james	2019/02/27 11:12:12	2019/02/27 11:12:12	Users	Users	Active
<input type="checkbox"/>	lily	2019/02/27 11:14:48	2019/02/27 11:12:55	Users		Locked
<input type="checkbox"/>	oliver	2019/02/27 11:13:14		Users		Unregistered

To unlock a TOTP user's account:

1. Go to the Users tab. The list of users is displayed.
2. Select the user whose account you choose to unlock.
3. Click on the **Unlock** button.

Auth Servers > TOTP_Local
TOTP_Local

Settings **Users**

Show users named: * Show 200 users **Update**

Unlock **Reset** Page 1 of 1 |< < > >|

	Username ▲	Last Attempted	Last Successful Login	User Information		
				Realm Registered From	Realm Last Logged In	Status
<input type="checkbox"/>	lorenz	2019/02/27 11:10:56	2019/02/27 11:10:56	Users	Users	Active
<input type="checkbox"/>	ursisian	2019/02/27 11:11:18		Users		Unregistered
<input type="checkbox"/>	emma	2019/02/27 11:16:36	2019/02/27 11:16:36	Users	Users	Active
<input type="checkbox"/>	james	2019/02/27 11:12:12	2019/02/27 11:12:12	Users	Users	Active
<input checked="" type="checkbox"/>	illy	2019/02/27 11:14:48	2019/02/27 11:12:55	Users		Locked

To reset a TOTP user's account:

1. Go to the Users tab. The list of users is displayed.
2. Select the user whose account you choose to reset.
3. Click on the **Reset** button. This removes the user entry from the table.

Auth Servers > TOTP_Local
TOTP_Local

Settings **Users**

Show users named: * Show 200 users **Update**

Unlock **Reset** Page 1 of 1 |< < > >|

	Username ▲	Last Attempted	Last Successful Login	User Information		
				Realm Registered From	Realm Last Logged In	Status
<input type="checkbox"/>	lorenz	2019/02/27 11:10:56	2019/02/27 11:10:56	Users	Users	Active
<input type="checkbox"/>	ursisian	2019/02/27 11:11:18		Users		Unregistered
<input type="checkbox"/>	emma	2019/02/27 11:16:36	2019/02/27 11:16:36	Users	Users	Active
<input checked="" type="checkbox"/>	james	2019/02/27 11:12:12	2019/02/27 11:12:12	Users	Users	Active

Viewing/Generating Backup Codes

To view/generate TOTP backup codes after successful login to a TOTP server via web:

1. User successfully authenticates to primary auth-server and TOTP auth-server via web.
2. Click on the Preference option on the top of the page.
3. In the Preference page, under TOTP Backup codes, click on either View or Generate to obtain user's TOTP backup codes.

Preferences

General

Change Password

Old Password:

New Password:

Confirm Password: Change Password Rectangular Step

TOTP Backup Codes

View Generate

VRUDW5 3YGM33
WY22PA JMHETQ
OR4ZU4 5CLOBF
KOUcBT MEBQ46
IM6TXX NH3PQD

Copy to Clipboard

Exporting/Importing TOTP Users

To export/import TOTP users:

1. Select **Authentication > Auth. Servers**.
2. Click the link for the authentication server you want to manage.
3. Click the Users tab to display the user accounts table. The user accounts table includes entries for the accounts that have been created.
4. Use the Export and Import buttons located at the bottom of the user accounts table to export and import TOTP users data.

Auth Servers > TOTP_Local

TOTP_Local

Settings **Users**

Show users named: Show 200 users Update

Unlock Reset Page 1 of 1 < > << >>

	Username	Last Attempted	Last Successful Login	User Information		
				Realm Registered From	Realm Last Logged In	Status
<input type="checkbox"/>	antti	2019/02/27 11:10:56	2019/02/27 11:10:56	Users	Users	Active
<input type="checkbox"/>	...	2019/02/27 11:11:18		Users		Unregistered
<input type="checkbox"/>	emma	2019/02/27 11:16:36	2019/02/27 11:16:36	Users	Users	Active
<input type="checkbox"/>	james	2019/02/27 11:12:12	2019/02/27 11:12:12	Users	Users	Active
<input type="checkbox"/>	illy	2019/02/27 11:55:25	2019/02/27 11:12:55	Users		Active
<input type="checkbox"/>	oliver	2019/02/27 11:13:14		Users		Unregistered
<input type="checkbox"/>	olivia	2019/02/27 11:16:05	2019/02/27 11:16:05	Users	Users	Active
<input type="checkbox"/>	william	2019/02/27 11:13:49	2019/02/27 11:13:49	Users	Users	Active

Page 1 of 1 < > << >>

Export Import

Configuring HTTP Attribute Server

IPS retrieves endpoint/user information and uses it for compliance assessments and role assignment. The configured HTTP attribute server has to be mapped as a "Device Attributes" under the realm configuration and role mapping rules can be used to assign the roles based on the attributes received from the attribute server.

To configure authentication with HTTP Attribute server:

1. Select **Authentication > Auth.servers**.
2. Select **HTTP Attribute Server** and click **New Server** to display the configuration page.
3. Enter the name of the server.
4. Select the required template from the drop down.
5. Enter the hostname/IP address of the third-party server.
6. Click **Test Connection** to validate the connection between IPS and third-party server (McAfee ePo/Nozomi Networks).
7. Save the configuration.

Auth Servers > New HTTP Attribute Server

New HTTP Attribute Server

* Name: Label to reference this server.

* Template: To manage templates, click [here](#)

* Host: IP Address/Hostname

Server Certificate Validation: Enable this option to verify the server's certificate.

indicates required field

Cascading Authentication Support

Cascading multiple external authentication servers provides a continuous, reliable process for authenticating and authorizing external users. If authentication fails on the first authentication server, then IPS attempts to authenticate the user by using the subsequent external authentication server configured in the realm under the sign-in policy page. The fallback mechanism continues until the user is successfully authenticated or there is no available realm. This feature is supported for Native Supplicant 802.1x and non EAP (like PAP, CHAP) RADIUS usecase.

To configure cascading authentication support:

1. Select **Authentication > Auth.servers** and create auth server. For example, AD or RADIUS server.
2. Select **Signing in > Sign-in Policies**. Arrange the realms in the desired order. The fallback authentication is based on this order.
3. Enable **Fallback to next available realm if authentication fails** option for user or admin users.

Signing In > Sign-in Policies > */

*/

User type: Users Administrators

Sign-in URL: Format: <host>/<path>/, Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: To create or manage pages, see [Sign-In pages](#).

▼ Authentication realm

Specify what realms will be available when signing in.

<input type="checkbox"/>	Available realms	Authentication protocol set	
	<input type="text" value="Cert Auth"/> ▼	<input type="text" value="- Not applicable -"/> ▼	<input type="button" value="Add"/>
<input type="checkbox"/>	adrealm	802.1X	
<input type="checkbox"/>	ldaprealm	802.1X	
<input type="checkbox"/>	localrealm	802.1X	
<input type="checkbox"/>	sbrrealm	802.1X	
<input type="checkbox"/>	sqlrealm	802.1X	

If more than one realm appears above, the Policy Secure sign-in page will ask the user to choose. Other endpoints cannot choose a realm, the Policy Secure will assign the first suitable realm from the list. If no realms appear above, sign-in will fail.

Fallback to next available realm if authentication fails

User may specify the realm name as a Username suffix

4. Verify the Sign-in Policies page.

Signing In > Sign-in Policies

Sign-in Policies

Sign-in Policies | Sign-in Pages | Sign-in Notifications | Authentication Protocol Sets

Restrict access to administrators only
Only administrator URLs will be accessible across the cluster. Note that Administrators can attempt to sign in even if all rules on this page are disabled.
Warning: Enabling this option will immediately terminate all user sessions from all nodes across the cluster.

New URL... Delete... Enable... Disable... Save Changes

Administrator URLs	Sign-In Page	Authentication Realm(s)	Enabled	Realm Fallback Enabled
<input type="checkbox"/> */admin/	Default Sign-In Page	Admin Users	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User URLs	Sign-In Page	Authentication Realm(s)	Enabled	Realm Fallback Enabled
<input type="checkbox"/> */guestsponsor/	Default Sign-In Page	Guest Sponsor (NA)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> */guestadmin/	Default Sign-In Page	Guest Admin (NA)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> */certauth/	Default Sign-In Page	Cert Auth (Cert Auth)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> */	Default Sign-In Page	adrealm (802.1X), ldaprealm (802.1X), localrealm (802.1X), abrealm (802.1X), sqrealm (802.1X)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> */guest/	Default Sign-In Page	Guest (Guest)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> */test/	Default Sign-In Page	native realm (nativeprotocol), test (deviceauth), adrealm (802.1X), another (deviceauth)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Configuring MSSQL Server Accounting

IPS supports storing the RADIUS accounting information to an external SQL database. IPS offers SQL Accounting feature under Auth Servers. MSSQL accounting supported only for 802.1x use cases and only one SQL server can be configured.

- The SQL statement is completely user-specified, allowing support of existing tables with existing field names and formats. It can include a variety of arithmetic and string expressions.
- Stored procedures invoked by SQL accounting can make use of input parameters, record results, and return output parameters.

Radius Accounting Request (Start, Stop, Interim) is received in IPS from switch. Radius Accounting attributes are extracted, and the attributes configured in the SQL queries will be sent to the SQL server based on the realm configuration. Apart from RADIUS Accounting Request attributes, the attributes in the below table can also be used in the insert query.

Attribute Name	Datatype	Description
TransactionTime	Time	The date/time that the event occurred that is the subject of the request.
Time	Time	The date/time when the request is being processed. (This is later than TransactionTime if the request is a retry.)
Type	String	The RADIUS accounting request type.
NASAddress	IP address	The IP address of the requesting RAS.
NASName	String	The name of the network access device that originated the request. This may be the name of the RADIUS client entry in the database or the value of the NAS-Identifier or NAS-IP-Address attribute.
NASModel	String	The RAS make/model.
FullName	String	The full name of the logged in user.
AuthType	String	The method by which the user was authenticated.

Attribute Name	Datatype	Description
RADIUSClientName	String	The name of the network access device, as specified in a RADIUS client entry in the Steel-Belted Radius database.

Configuring SQL Accounting

You must configure both IPS and SQL database to support SQL accounting.

1. Select **Authentication** > **Auth.Servers** and select **SQL Auth Server**.
2. Select **Accounting** in configure SQL server.
3. Enter the SQL Accounting server settings as described in the table in the following steps.
4. Under SQL Accounting Queries, enable Use this Acct-Start statement for Acct-Stop and Acct-Interim to use the same Start statement for Acct-Start and Acct-Interim.

5. Click **Test Connection** to test the connectivity to the server.

6. Click **Save Changes**.

Settings	Guidelines
Name	Specify a name to identify the server within the system.
SQL Accounting Server	Specify the SQL Accounting server host name or IP address.
SQL Port	Specify the SQL port number through which the SQL Accounting server is accessed.
SQL Service Name	(Optional) Specify the SQL service name if SQL service name has been defined in the SQL Accounting server configuration.
Admin	Specify the administrator username.
Password	Specify the password.
Connection Timeout	Specify the connection timeout value from 5 to 60 seconds. If this time is exceeded, and if there is a backup server defined, then the device attempts to reach the backup server.
Search Timeout	Specify the search timeout value from 5 to 60 seconds. It specifies the maximum amount of time the device will wait for the SQL Accounting server to return search results.
Use SSL	Select Use SSL to establish an encrypted connection between the client and server.
Server Certificate Validation	Select this option to validate the server certificate before using the public and private keys for encryption/decryption.

Auth Servers > SPAccountingServer > Settings

Settings

Settings Users

*Configure SQL Server: Auth Accounting

*Name: SPAccountingServer Label to reference this server.

*SQL Accounting Server: 10.10.10.10 Name or IP address

*SQL Port: 1433

SQL Service Name: spaccounting SQL Service/Database Name

*Admin: test

*Password: *****

*Connection Timeout: 15 Seconds to wait for connection to SQL Auth server (Min 5, Max 120)

*Search Timeout: 15 Seconds to wait for search results, excluding connection time (Min 5, Max 120)

Use SSL:
Server Certificate Validation:

SQL Accounting Queries

Use this Acct-Start Statement for Acct-Stop and Acct-Interim.

*Acct-Start Statement: [CALL shrsiq_start_sp('Acct-Session-Id', 'Acct-Status-Type', 'Service-Type', 'Acct-Status-Type', 'Service-Type', 'Acct-Status-Type')] example: INSERT INTO accounting (TransTime, NASName, Type, PacketsIn, PacketsOut) VALUES (:TransactionTime, :NASName, :Type, :Acct-Input-Packets, :Acct-Output-Packets)

Acct-Stop Statement: [CALL shrsiq_stop_sp('Acct-Session-Id', 'Acct-Status-Type', 'Service-Type', 'Acct-Status-Type', 'Service-Type', 'Acct-Status-Type')] example: INSERT INTO accounting (TransTime, NASName, Type, PacketsIn, PacketsOut) VALUES (:TransactionTime, :NASName, :Type, :Acct-Input-Packets, :Acct-Output-Packets)

Acct-Interim Statement: [CALL shrsiq_intermediate_sp('Acct-Session-Id', 'Acct-Status-Type', 'Service-Type', 'Acct-Status-Type', 'Service-Type', 'Acct-Status-Type')] example: INSERT INTO accounting (TransTime, NASName, Type, PacketsIn, PacketsOut) VALUES (:TransactionTime, :NASName, :Type, :Acct-Input-Packets, :Acct-Output-Packets)

Test Connection

Save Changes Reset

* Indicates required field.

7. Under **User Realms > Users**, select the SQL Accounting server.

User Realms > Users > General

General | Authentication Policy | Role Mapping

* Name: Label to reference this realm

Description:

Default authentication realm for users

When editing, start on the Role Mapping page

▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Specify the server to use for authenticating users.

User Directory/Attribute: Specify the server to use for authorization.

Accounting: Specify the server to use for Radius accounting.

Device Attributes: Specify the server to use for device authorization.

Datum	Type	NASAddress	NASName	User-Name	NAS-IP-Address	NAS-Port	NAS-Identifier	Acct-Status-Type	Acct-Session-Id
1	2021-06-20 22:12:31	1	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	1	000D00000162
2	2021-06-20 22:13:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
3	2021-06-20 22:14:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
4	2021-06-20 22:15:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
5	2021-06-20 22:16:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
6	2021-06-20 22:17:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
7	2021-06-20 22:18:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
8	2021-06-20 22:19:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
9	2021-06-20 22:20:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
10	2021-06-20 22:21:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
11	2021-06-20 22:22:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
12	2021-06-20 22:23:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
13	2021-06-20 22:24:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
14	2021-06-20 22:25:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
15	2021-06-20 22:26:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
16	2021-06-20 22:27:31	3	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	3	000D00000162
17	2021-06-20 22:27:34	2	10.0.0.3.41	client_2	10.0.0.41	2	PPS...tion-HP-2920	2	000D00000162

```

EAM24460 2021-07-01 09:20:08 - ic - [10.96.202.1] PPS...[Users][Users] - Received a RADIUS Accounting Stop request. Terminated session
AUT31643 2021-07-01 09:20:08 - ic - [10.96.202.1] PPS...[Users][Users] - IP Address 10.0.0.41 has been released for the user PPS...[Users]
SBR31642 2021-07-01 09:11:16 - ic - [127.0.0.1] PPS...[Users][Users] - User PPS...[Users] has been assigned IP address
AUT31643 2021-07-01 09:11:16 - ic - [10.96.202.1] PPS...[Users][Users] - IP Address 10.0.0.41 has been released for the user PPS...[Users]
EAM24805 2021-07-01 09:11:16 - ic - [127.0.0.1] PPS...[Users][Users] - RADIUS authentication accepted for PPS...[Users] (realm 'Users') from location-group 'Default' and attributes are: NAS-IP-Address = 10.0.0.41,NAS-Port = 2,NAS-Port-Type = 15
    
```

The following is an example of a SQL INSERT statement in IPS-SQL Accounting query. The insert statement will directly provide the attributes and value placeholders to be saved on the SQL database.



For SBR-E customers, the "%" and "@" symbols in the insert query should be replaced with ":" symbol and the format specifiers should be removed.

```
INSERT INTO shrisql_start("Acct-Session-Id", "Acct-Status-Type", "Service-Type", "Acct-Authentic", "NAS-Port", "Calling-Station-Id", "Called-Station-Id", "NAS-Port-Type", "NAS-IP-Address", "NAS-Identifier", "User-Name", "MS-RAS-Vendor", "Acct-Delay-Time", "Framed-IP-Address", "TransactionTime", "Time", "NASAddress", "NASName", "NASModel", "FullName", "AuthType", "RADIUSClientName") VALUES (:Acct-Session-Id, :Acct-Status-Type, :Service-Type, :Acct-Authentic, :NAS-Port, :Calling-Station-Id, :Called-Station-Id, :NAS-Port-Type, :NAS-IP-Address, :NAS-Identifier, :User-Name, :MS-RAS-Vendor, :Acct-Delay-Time, :NASAddress, :TransactionTime, :Time, :NASAddress, :NASName, :NASModel, :FullName, :AuthType, :RADIUSClientName)
```

Stored Procedure Example

The following is an example of stored procedure configuration to insert an entry to the SQL table.

```
{CALL shrisql_start_sp(:Acct-Session-Id, :Acct-Status-Type, :Service-Type, :Acct-Authentic, :NAS-Port, :Calling-Station-Id, :Called-Station-Id, :NAS-Port-Type, :NAS-IP-Address, :NAS-Identifier, :User-Name, :MS-RAS-Vendor, :Acct-Delay-Time, :NASAddress, :TransactionTime, :Time, :NASAddress, :NASName, :NASModel, :FullName, :AuthType, :RADIUSClientName)}
```

Stored Procedure syntax on MSSQL Server

The following is an example of a stored procedure syntax on MSSQL server.

```
CREATE PROCEDURE shrisql_start_sp
    (@AcctSessionId varchar(40), @AcctStatusType varchar(40), @ServiceType varchar(40), @AcctAuthentic varchar(40),
    @NASPort varchar(40), @CallingStationId varchar(40), @CalledStationId varchar(40), @NASPortType varchar(40), @NASIPAddress varchar(40),
    @NASIdentifier varchar(40), @UserName varchar(40), @MSRASVendor varchar(40), @AcctDelayTime varchar(40), @FramedIPAddress varchar(40),
    @TransactionTime varchar(40), @Time varchar(40),
    @NASAddress varchar(40), @NASName varchar(40), @NASModel varchar(40), @FullName varchar(40), @AuthType varchar(40), @RADIUSClientName varchar(40))
AS
BEGIN
    SET NOCOUNT ON
    INSERT INTO shrisql_start ([Acct-Session-Id], [Acct-Status-Type], [Service-Type], [Acct-Authentic], [NAS-Port], [Calling-Station-Id],
    [Called-Station-Id], [NAS-Port-Type], [NAS-IP-Address], [NAS-Identifier], [User-Name], [MS-RAS-Vendor], [Acct-Delay-Time], [Framed-IP-Address],
    [TransactionTime], [Time],
    [NASAddress], [NASName], [NASModel], [FullName], [AuthType], [RADIUSClientName])
    VALUES (@AcctSessionId, @AcctStatusType, @ServiceType, @AcctAuthentic, @NASPort, @CallingStationId,
    @CalledStationId, @NASPortType, @NASIPAddress, @NASIdentifier, @UserName, @MSRASVendor, @AcctDelayTime,
    @FramedIPAddress, @TransactionTime, @Time,
    @NASAddress, @NASName, @NASModel, @FullName, @AuthType, @RADIUSClientName)
END
```

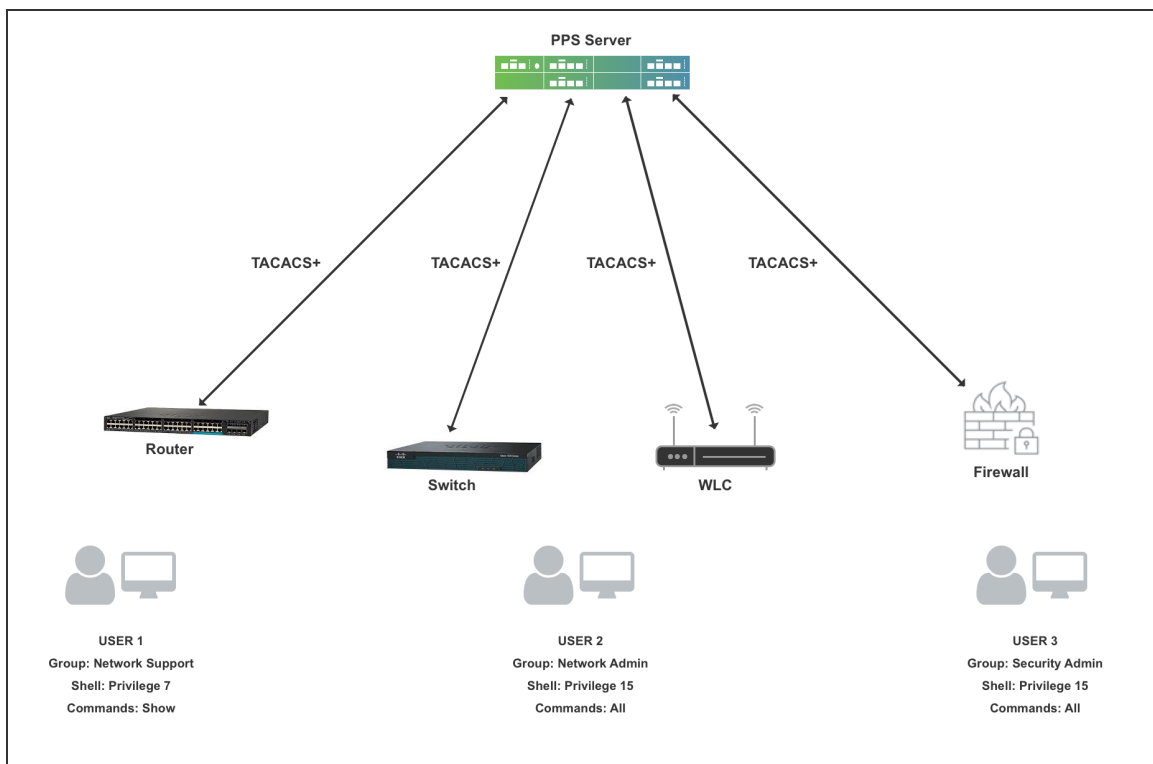
Network Device Administration using TACACS+

Overview

The network device administrators are required to configure and maintain the network devices such as switches, wireless access points, routers, and gateways. IPS supports configuring and coordinating the network devices through IPS Admin UI.

The administrator implements policies to determine who can login to a network device console, telnet session, secure shell (SSH) session to manage each device, what level of privilege do they have, what operations they can run (that is, the commands the admin user is permitted to run on the device) and also audit all the actions taken.

Managing these policies separately on each device is not just unmanageable but can lead to security incidents or errors that result in loss of service and network downtime due to undesired access. Most compliance requirements and security standards require using standardized tools to centralize authentication for administrative management.



The above deployment consists of 3 types of administrators:

- **User1** - This admin belongs to Network Support Group and can only access show commands on router, switches and access points. The admin has no access to Firewall.
- **User2** - This admin belongs to Network Admin Group and can access all commands on routes, switches and access points. The admin has no access to Firewall.
- **User3**- This admin belongs to Security admin group and an firewall administrator and does not have access to routers, switches and access points.

A large company will have many devices from different vendors. It requires administrators to manage the network with many hierarchical levels.

Without a centralized server for administration, every time a new device is deployed, several admin accounts needs to be created on the new device to assign the required privilege for each of the admin. Similarly, if a new admin onboards an functional organization, the account needs to be created on thousands of devices.

With Ivanti Policy Secure(IPS) acting as a centralized server for device administration using TACACS+, a new admin can just be mapped to required group. A new Admin account can be configured either locally on IPS or any external servers such as AD, LDAP and so on. Similarly, when a new device is purchased, the only configuration is configuring IPS as a centralized server for device administration on device.

Licensing

TACACS+ user login does not consume any user license however either POLSEC license or Profiler license is required to be installed.

Authentication

Provides complete control of authentication through login and password.

Authorization

Provides fine-grained control over user capabilities for the duration of the user's session, which includes idle time-out, session duration. You can enforce restrictions on what commands a user may execute by configuring the privilege level for administrators. Within the privilege-level, further control can be forced by specifying command or regex match.

Ivanti Policy Secure(IPS) supports 2 types of authorization techniques for administrators:

- Exec authorization- This determines a user's privilege level when they are authenticated. The admins can run the commands, which are allowed in the user's privilege level.
- Command authorization- TACACS+ command authorization provides centralized control of the commands available to IPS admin user. In this, every command is sent to IPS for authorization and command is permitted after getting authorized by IPS.
 - A Telnet, SSH, or console interface user who is previously authenticated by IPS using TACACS+ enters a command on the device.
 - The network device looks at its configuration to see if the command is at a privilege level that requires TACACS+ command authorization.
 - If the command requires authorization, the device consults the IPS to see if the user is authorized to use the command.
 - If the user is authorized to use the command, the command is executed.

Accounting

Collects and sends information used for auditing to the TACACS+ server. Network device administrators can use the accounting facility to track user activity for a security audit or to provide information for user billing. Accounting records include user identities, start and stop, executed commands.

Configuration

Configuring Admin Role

Admin role enables you to define granular administrative access privileges. For example, an organization would require multiple admin roles with different privilege levels to ensure protection from sensitive company information.

To create an Admin role for TACACS+:

1. Select **Administrators > Admin Roles > New Admin Role**. Enter a role name. You can create multiple admin roles with different privilege levels. For example, tac_admin_role.

Admin Roles > tac_admin_role > General > Overview

Overview

General System Users Administrators Resource Policies

Overview Restrictions Session Options UI Options

Name:

Description:

[Save Changes](#)

Options

Session and appearance options are specified in [Default Options](#). Check the following if this role should override these defaults.

- Session Options ([Edit](#))
- UI Options ([Edit](#))

2. Under Session Options, specify the following attributes:

- **Idle Time-out** - If no input is received or sent in the period specified, the session is disconnected.
- **Max session length**- It specifies the maximum length of time that the session can exist. After this value has expired, the session gets disconnected.

Admin Roles > tac_admin_role > General > Session Options

Session Options

General System Users Administrators Resource Policies

Overview Restrictions **Session Options** UI Options

[Save Changes](#)

Session lifetime

*Idle Timeout: minutes (min: 5)

*Max. Session Length: minutes (min: 6)

Configuring Admin Realm

An authentication realm defines the authentication server with which end user is authenticated and the list of restrictions that must be satisfied on the client machine during sign-in. It also provides role mapping option to administrators for configuring the list of roles that needs to be assigned to the user. Role mapping provides flexibility to administrators in configuring how different set of roles need to be assigned to the user.

An admin can configure multiple admin realms when different authentication servers are required for authentication for different devices. Admin's can also use different backend servers for managing different device groups.

Create an Authentication realm and then associate the authentication server to it.

1. Select **Administrators > Admin Realms > New Authentication Realm**.
2. Under Servers, specify the Authentication server (AD, LDAP, Local, or RSA (ACE Server)). For more information, see AAA Servers.

Admin Realms > tac_admin_realm > General

General

General Authentication Policy Role Mapping

Name: tac_admin_realm Label to reference this realm

Description:

When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: System Local Specify the server to use for authenticating users.

Directory/Attribute: None Specify the server to use for authorization.

Accounting: None Specify the server to use for Radius accounting.

Dynamic policy evaluation

Enable dynamic policy evaluation


Other Settings

Authentication Policy: None Password restrictions: 1 Rule

Role Mapping: None

Save Changes

3. Configure any Admin role restrictions. For example, Source IP restriction.

 Browser, Host Checker, Certificate restrictions are not supported with TACACS+.

Admin Roles > tac_admin_role > General > Restrictions > Source IP



Source IP

General System Users Administrators Resource Policies

Overview **Restrictions** Session Options UI Options

Source IP Browser Certificate Host Checker

Allow users to sign in from any IP address
 Allow or deny users from the following IP addresses:

Delete  

<input type="checkbox"/>	IPv4/v6 Address	Netmask/Prefix Length	Allow/Deny	
	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> Allow <input type="radio"/> Deny	<input type="button" value="Add"/>
<input type="checkbox"/>	10.204.89.239	255.255.255.0	Allow	

Note: This restriction will not allow access to the role if no IP addresses are listed. Add one or more source IP addresses from which users are allowed to sign in or denied access.

- Set the role mapping rules. For example, create a rule to assign all users with username as tac_user to tac_admin_role.

Admin Realms > tac_admin_realm > Role Mapping > Role Mapping Rule

Role Mapping Rule

Rule based on: Username

* Name:

▼ Rule:if username...

is If more than one username should match, enter one username per line. You can use * wildcards.

▼ then assign these roles

Available Roles: Administrators, Read-Only Administrators

Selected Roles: tac_admin_role

Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

Admin Realms > tac_admin_realm > Role Mapping

Role Mapping

General Authentication Policy **Role Mapping**

Specify how to assign delegated admin roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/>	1. username is "tac_user"	→ tac_admin_role	tac_rule	

When more than one role is assigned to a user:

- Merge settings for all assigned roles
- User must select from among assigned roles
- User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

i Role mapping rule execution is based on the order of the rules.

Configuring Device Group

The device groups are created in a heterogeneous network where there are devices from multiple vendors with different command set. Devices with same command syntax are grouped so that it is easy to manage. IPS considers each group as a single unit while applying the shell policies.

For example, if your deployment has devices from multiple vendors, you can group them into multiple device groups based on their command syntax. Similarly, you can also create different device groups based on whether the device is a WLC/Switch.

To create a device group:

1. Select **Endpoint Policy > Network Device Administration > Device Group**.
2. Enter the name and description of the device group
3. Associate the previously created Admin Realm with the device group.
4. A device group policy logically groups network devices by associating the devices with specific admin realm.
5. Click **Save Changes**.

The screenshot shows the configuration page for a device group named 'tacacs_device'. The breadcrumb navigation is 'Network Device Administration > Device Group > tacacs_device'. The page title is 'tacacs_device'. Under the 'Device Group' section, there are three fields: '* Name:' with the value 'tacacs_device' and a tooltip 'Label to reference this Device Group.', 'Description:' which is empty, and '* Admin Realm:' with a dropdown menu showing 'tac_admin_realm' and a tooltip 'To manage realm, see the Admin Realms'. At the bottom left, there is a blue 'Save Changes' button.

Configuring TACACS+ Client

A TACACS+ client policy specifies the information required for the device to connect to Ivanti Policy Secure for admin access control. You can add the network devices as TACACS+ clients for the administrator to manage. IPS allows you to configure an IP address range for TACACS+ clients.

To create a TACACS+ client:

1. Select **Endpoint Policy > Network Device Administration > TACACS+ Clients > New TACACS+ Client**.
2. Enter a name for the TACACS+ client.

3. Enter a description.
4. Enter the IP address of the client.
5. Enter the IP address range for the TACACS+ clients.
6. Enter the shared secret.
7. Select the device group from the drop down.
8. Under TACACS+ Advance Settings, enable/disable allow authorization without authentication.
9. Click **Save Changes**.

Network Device Administration > TACACS+ Client > New TACACS+ Client

New TACACS+ Client

▼ TACACS+ Client

* Name: Label to reference this TACACS+ Client.

Description:

* IP Address: IP Address of this TACACS+ Client.

* IP Address Range: Number of IP Addresses for this TACACS+ Client

* Shared Secret: TACACS+ shared secret

* Device Group: To manage groups, see the Device Group

▼ TACACS+ Advance Settings

Allow Authorization (w/o authentication) Allow Authorization (w/o authentication)

Save Changes

* Indicates required field



Ivanti Policy Secure(IPS) does not support adding IPv6 TACACS+ clients.

Configuring Shell Policies

Define the Policies for the Admin Role and the corresponding Device Group. The Policies should be mapped with the selected Admin Roles and the Device Group.

To configure shell policies:

1. Select **Endpoint Policy > Network Device Administration > Shell Policies**.
2. Enter the name of the policy.

3. Enter the description.
4. Under Device Group, select the **Device Group**.
 - **Policy Applies to all groups**- If you select this option, the shell policy is applied to all the device groups.
 - **Policy Applies to selected groups**- If you select this option, the shell policy is applied only to the selected device group.
5. Under Shell Policy, specify the following:
 - Enter the Default Privilege level.
 - Maximum Privilege level (1-15).
 - (Optional) Service- The default value is "shell". Admin can explicitly configure specific service type.
6. Under Command Set, Enter the command, arguments, and the action (permit/deny) for the Admin. If it doesn't match any rule it takes the default action:
 - **Deny** any command that does not hit any of the rule
 - **Permit** any command that does not hit any of the rule
7. Command authorization is supported on most of the switches such as HP and Cisco. However, devices such as F5 and Juniper does not support individual command authorization with TACACS+ server due to the delay in command execution. For F5 and Juniper devices the required set of commands are mapped to different roles locally as the roles are predefined. The TACACS+ server sends the desired role through the custom attributes during user authentication.

Under **Custom Attributes**, enter the Attribute name, value, and specify the requirement as either mandatory or optional. Click **Add**.

Mandatory arguments require that the client must understand the attribute and act upon it otherwise the authentication fails.

8. Under Roles, select the Admin Role.

- **Policy Applies to all roles**- If you select this option, the shell policy is applied to all the admin roles.
- **Policy Applies to selected roles**- If you select this option, the shell policy is applied only to the selected admin role.
- **Policy Applies to all roles other than the selected role**- If you select this option, the shell policy is applied to all the admin roles other than the selected role.

9. Click **Save Changes**.

Network Device Management > Shell Policies > networkadmin

networkadmin

▼ New Shell Policy

* Name: Label to reference this policy.

Description:

▼ Device Group

Policy applies to ALL groups
 Policy applies to SELECTED groups

Available Device Groups:

Selected Device Groups:

▼ Shell Policy

* Default Privilege: Shell Privilege Levels supported

* Maximum Privilege:

Service: This is optional and default service is 'shell'

▼ Command Set

Command	Arguments	Action	
<input type="text"/>	<input type="text"/>	<input type="text" value="permit"/>	<input type="button" value="Add"/>

Deny any command that does not hit any of the rule in the table above
 Permit any command that does not hit any of the rule in the table above

▼ Custom Attributes

Attribute	Value	Requirement	
<input type="text"/>	<input type="text"/>	<input type="text" value="Mandatory"/>	<input type="button" value="Add"/>
<input type="checkbox"/> local-user-name	network-admin	Mandatory	
<input type="checkbox"/> user-permissions	view	Mandatory	
<input type="checkbox"/> deny-commands	show firewall\$	Mandatory	
<input type="checkbox"/> allow-commands	edit*	Mandatory	

▼ Roles

Policy applies to ALL roles
 Policy applies to SELECTED roles
 Policy applies to all roles OTHER THAN those selected below

Available roles:

Selected roles:

* indicates required field

The below page is displayed after configuring the shell policy using command set.

Network Device Management > Shell Policies

Shell Policies

Device Groups | TACACS+ Clients | **Shell Policies**

New Policy Duplicate Delete Save Changes

10 records per page

	Name	Device Group	Default Privilege	Maximum Privilege	Command Set	Custom Attributes	Applies to
1	helpdeskadmin	Cisco switches	3	4	Denied Commands		helpdeskadmin
2	superadmin	Cisco switches	15	15			superadmin
3	networkadmin	Juniper	3	4	Denied Commands	Mandatory Attributes local-user-name=network-admin user-permissions=view,view-configuration allow-commands=configure * deny-commands=show firewall\$	networkadmin
4	readonly	Juniper	15	15		Mandatory Attributes Optional Attributes	readonly

TACACS+ Command Sets

Command sets consists of a specific list of commands that can be executed by a network device administrator. IPS determines whether the administrator is authorized to execute these commands based on the privilege level configuration.

Regex (Wildcards)

A command line comprises the command and zero or more arguments. When IPS receives a command line (request), it handles the command and its arguments in different ways. It matches the command in the request with the command specified.

For example, Show device-[a-z]* st[a-z]*us

This command has 2 arguments.

- Argument 1 – device-[a-z]*
- Argument 2 – st[a-z]*us

The command arguments in the request are taken based on the order. After the command and arguments match to any of the command set based on the order corresponding action (permit/deny) is taken by IPS.

If command doesn't match with the any of the command set configured then default action will be taken. The default action taken can be:

- Deny any command that does not hit any of the rule
- Permit any command that does not hit any of the rule

Multiple command Sets

Ivanti Policy Secure(IPS) checks all the commands in the command set sequentially for the first match.

It compares the command name from the network device with the exact command configured in the command set.

If the command matches and there are no arguments from device group

- If there are no arguments to match from device as well as no arguments configured, then the command set is considered as match.
- If there are no arguments from device group but arguments are configured, then it's a no match.
- If arguments are sent by device group, then it is compared with regex pattern configured in arguments of the command set.

If argument is matched, then command set is considered as a match, and corresponding action is taken.

- If the first match has action as Permit, IPS designates the command set as Permit.
- If the first match has Deny, IPS designates the command set as Deny.

If the command doesn't match with any of the command set configured one of the below default action is taken.

Ivanti Policy Secure(IPS) checks all the commands in the command set sequentially for the first match.

- Deny any command that does not hit any of the rule.
- Permit any command that does not hit any of the rule.

If there are many profiles, then the first matching profile is applied.

Monitoring Device Administration

Ivanti Policy Secure(IPS) provides various logs that allow you to view information related to accounting, authorization, and command accounting of devices configured with TACACS+.

General recommendation – For recovery purposes, it is suggested to have a local backup account. The console login should be redirected to local.

To monitor device administration:

Select **System > Log Monitoring > Admin Access**:

- To enable Accounting, you must click the checkbox for **TACACS+ Accounting messages**.
- To enable authorization, you must click the checkbox for **TACACS+ Authorization messages**.

Log/Monitoring > Admin Access > Log settings

Log settings

Events | User Access | **Admin Access** | Sensors | Client Logs | SNMP | Statistics | Advanced Settings

Log | **Settings** | Filters

Save Changes | Reset

▼ Maximum Log Size

Max Log Size: MB

Note: To archive log data, see the [Archiving](#) page.

▼ Select Events to Log

Administrator changes License Changes

TACACS+ Accounting messages TACACS+ Authorization messages

Administrator logins

▼ Syslog Servers

Troubleshooting

Ivanti Policy Secure(IPS) provides logging and monitoring capabilities to help you track events and user activities. The system generates event logs related to system performance, administrator actions, network communications, access management framework results, user sessions, and so forth.

The available logs, includes:

- Event Logs- This file contains a variety of system events, such as session timeouts, systems errors and warnings, server restart notifications and connectivity requests.
- Admin Access Logs- This file contains administration information, including administrator changes to user, system and network settings, such as changes to session timeouts, license changes and so on.

TACACS+ Event and Admin Logs

Event Logs

1. Logging when count of TACACS+ connection reached system limit.

Minor – Limit of <max count> TACACS+ concurrent users reached

Minor	TAC31628	2018-01-31 14:40:48 - ic - [127.0.0.1] System()[] - Limit of 2 TACACS+ concurrent users reached
-------	----------	---

2. Dropping the incoming TACACS+ connection because received from unknown host.

Major - TACACS+ request received from unknown TACACS+ client <switch IP>

Major	TAC31629	2018-01-31 14:37:54 - ic - [127.0.0.1] System()[] - TACACS+ request received from unknown client 10.204.89.239
-------	----------	--

3. Dropping the incoming TACACS+ connection due to shared-secret mismatch.

Minor - Invalid TACACS+ packet from <switch IP>, discarding.

Minor	TAC31628	2018-01-31 14:35:58 - ic - [127.0.0.1] System()[] - Invalid TACACS+ packet from 10.204.89.239, discarding. Incorrect shared secret
-------	----------	--

Admin Access Logs

1. Exec Authorization [Only when Authorization is enabled under authorization setting]

- Log for exec authorization success

TACACS+ Shell authorization successful for <user> on switch-<switch ip> and attributes are: privilege = %d, idle-timeout = %d, session-timeout = %d

Info	TAC31611	2018-01-30 18:59:03 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm) [tac_admin_role] - 'TACACS+ Shell authorization successful for tac_user on 10.204.89.239 and attributes are: privilege = 15, idle-timeout = 5, session-timeout = 60'
------	----------	---

- Log for exec authorization failure due to no shell policy assigned to roles.

TACACS+ Shell authorization rejected for <user> on switch-<switch ip>. Reason- %s

Reasons-

- No session found
- No Shell policy found for the assigned roles

Info	TAC31612	2018-01-30 19:06:45 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm)[tac_admin_role] - 'TACACS+ Shell authorization rejected for tac_user on 10.204.89.239. Reason: No Shell policy found for the assigned roles'
------	----------	---

2. Command authorization [Only when Authorization is enabled under authorization setting]

- Log for command authorization success.

TACACS+ Authorization successful for command-%s from <user> on switch-<switch ip>

Info	TAC31611	2018-01-30 19:08:14 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm)[tac_admin_role] - 'TACACS+ Authorization successful for command-'show version' from tac_user on 10.204.89.239'
------	----------	---

- Log for command authorization failure due to no shell policy assigned to roles or due to deny under command set.

TACACS+ authorization rejected for command-<cmd> from <user> on switch-<switch ip>. Reason- %s

Reasons-

- No session found
- No Shell policy found for the assigned roles

Info	TAC31612	2018-01-30 19:37:02 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realms)[tac_admin_role] - 'TACACS+ authorization rejected for command-'show version' from tac_user on 10.204.89.239. Reason- No session found'
------	----------	--

- Matched with the rule – [command = %s, Arguments = %s, action = %s] in shell policy-%s

Info	TAC31612	2018-01-30 19:11:31 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realms)[tac_admin_role] - 'TACACS+ authorization rejected for command-'menu ' from tac_user on 10.204.89.239. Reason- Matched with the rule – [command = menu, Arguments = null, action = deny] in shell policy-tacacs_policy'
------	----------	--

- No match found. Default action is deny in shell policy-%s

Info	TAC31612	2018-01-30 19:12:31 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realms)[tac_admin_role] - 'TACACS+ authorization rejected for command-'display arp' from tac_user on 10.204.89.239. Reason- No match found. Default action is 'deny' in shell policy-tacacs_policy'
------	----------	---

3. Login Authentication: [Only when Administrator login is enabled under admin access setting]

- Login Success

Info	AUT30684	2018-01-30 18:59:02 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm)[] - Primary authentication successful for tac_user/System Local from 10.204.59.223(Shell login to 10.204.89.239).
------	----------	--

- Login failure due to authentication failure.

	AUT23458	2018-01-30 19:15:10 - ic - [10.204.59.223] tac_user(tac_admin_realm)[tac_admin_role] - Login failed using auth server System Local (Local Authentication). Reason: Failed
--	----------	---

- Login failure due to restrictions.

Info	AUT23458	2018-01-30 19:04:23 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm)[tac_admin_role] - Login failed. Reason: No Roles
------	----------	---

- Login failure due to no role available.

Info	AUT23458	2018-01-30 19:04:23 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm)[tac_admin_role] - Login failed. Reason: No Roles
------	----------	---

- Session deletion due to accounting stop received

Info	AUT31627	2018-01-30 19:23:43 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm)[tac_admin_role] - 'Received a TACACS+ Accounting stop request. Terminated Session.'
------	----------	--

- Session deletion due to session timeout.

Info	ADM20664	2018-01-30 19:34:40 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm)[tac_admin_role] - Session timed out for tac_user/tac_admin_realm due to inactivity (last access at 19:29:38 2018/01/30). Idle session identified during routine system scan.
------	----------	---

4. Enable Authentication: [Only when Administrator login is enabled under admin access setting]

- Enable authentication success.

Info	AUT30684	2018-01-30 19:28:09 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm)[] - Enable Service authentication successful for tac_user/System Local from 10.204.59.223(Shell login to 10.204.88.10).
------	----------	--

- Login failure due to authentication failure.

Info	AUT23458	2018-01-30 19:29:44 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm)[tac_admin_role] - Login failed using auth server System Local (Local Authentication). Reason: Failed
------	----------	---

- Login failure due to restrictions.

Info	AUT23458	2018-01-30 19:31:15 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm)[tac_admin_role] - Login failed. Reason: No Roles
------	----------	---

- Login failure due to no role available.

Info	AUT23458	2018-01-30 19:31:15 - ic - [xx.xxx.xx.xxx] tac_user(tac_admin_realm)[tac_admin_role] - Login failed. Reason: No Roles
------	----------	---

5. Assigning custom attributes from IPS to TACACS+ client (Juniper, F5)

Info	TAC31778	2019-04-23 11:55:11 - IPS- [127.0.0.1] user7(Admin realm) [networkadmin] - User assigned TACACS+ attribute(s) (local-user-name=network-admin user-permissions=view deny-commands=show firewall\$ allow-commands=edit*)
------	----------	--

Once the session is established the session is seen as TACACS+ Session in the Active Users Page

Status > Active Users

Active Users

Activity Overview **Active Users** Device Profiles Admin Notification

Show users named: * Show 200 users Update

Delete Session... Delete All Sessions... Refresh Roles Disable All Users...

Number of Users: 3

	User	Realm	Roles	Signed in	Signed in IP	MAC Address	Device Details	Agent Type	Agent Version	Endpoint Security Status
<input type="checkbox"/>	admin	Admin Users	Administrators	2018/3/29 10:15:41	172.21.16.225			Mac OS 10.12 Google Chrome		Not Applicable
<input type="checkbox"/>	admin1	Admin Users	Administrators	2018/3/30 12:42:13				Windows 8.1 Google Chrome		Not Applicable
<input type="checkbox"/>		tac_admin_realm	tac_admin_role	2018/3/30 13:06:07				TACACS+ Session		Not Applicable

Appendix

The following example shows how to configure the switch to authenticate and account using TACACS+.

Output 1: Example: Cisco iOS

```

**Authentication
aaa authentication login default group <group-name> local
aaa authentication enable default group <group-name> enable

**Authorization
aaa authorization exec default group <group-name> local
aaa authorization commands <privilege no.> default group <group-name> local
aaa authorization config-commands

**Accounting
aaa accounting exec default start-stop group <group-name>
aaa accounting commands <privilege no.> default start-stop group <group-name>
aaa accounting send stop-record authentication failure

```

**Mapping TACACS+ server IP to group

```

aaa group server tacacs+ <group-name>
server-private <server-ip> key <shared-secret>

```

Output 2: Example: HP switch

```

tacacs-server host <host-ip> key <shared-secret>
aaa authentication telnet login tacacs
aaa authentication telnet enable tacacs
aaa authentication login privilege-mode
aaa accounting exec start-stop tacacs

```



HP switches should be set with privilege level always. Enable authentication is not supported.

Output 3: Example: Juniper Switch


```

root@ex-2200# show system login
class class1 {
    idle-timeout 20;
}
class network-admin {
    idle-timeout 10;
}
user network-admin {
    uid 2002;
    class network-admin;
}
user remote-read-only {
    full-name "User template for remote read-only";
    uid 2014;
    class read-only;
}
user remote-super-users {
    full-name "User template for remote super-users";
    uid 2013;
    class super-user;
}
#show system tacplus-server
<IPS-IP> {secret "fkfljsfjsafjsaf"; }
#show system accounting
events [events];
#show system tacplus-options
service-name shell;

```

For more information on Juniper, see Juniper documentation.

Output 4: Example: F5 Device

Label	Sample Configuration
TACACS+ Authentication	https://support.f5.com/csp/article/K8811  Configure Service Name as "shell" instead of "ppp" under configuration for TACACS+ authentication.

Label	Sample Configuration
TACACS+ Accounting	https://support.f5.com/csp/article/K13762
Remote Role configuration using Custom attributes	https://devcentral.f5.com/Portals/0/Cache/Pdfs/2807/tacacs-remote-role-configuration-for-big-ip.pdf

Output 5: Example: Arista Switch

```

tacacs-server host <IPS-IP Address> key <secret-key>
!
aaa group server tacacs+ <group-name>
    server <IPS-IP Address>
!
aaa authentication login default local group tacacs+ group <group-name>
Required for enabling service authentication.
aaa authentication enable default group tacacs+ group <group-name> local
aaa authorization exec default local group tacacs+ group <group-name>
aaa authorization commands all default local group tacacs+ group <group-name>
aaa accounting exec default start-stop group tacacs+ group <group-name>
aaa accounting commands all default start-stop group tacacs+ group <group-name>
For Command based Authorization configure the following command.
aaa authorization commands all default group tacacs+ group <group-name>

For Role based Authorization configure the following command.
configure aaa authorization commands all default local
    
```

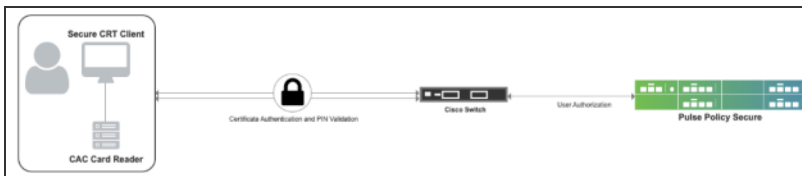
From the IPS Admin UI configure the custom attribute for Role based authorization as shown below.

Attribute	Value	Requirement
roles	network-operator	Mandatory

Two-Factor Authentication using Smart Cards

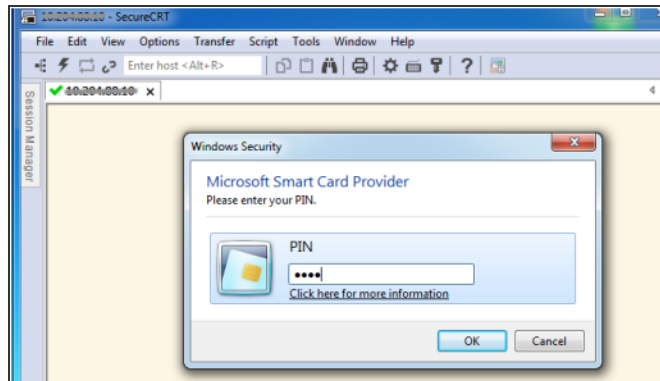
With growing digital world, effectively combating cybersecurity threats has become a major challenge. The scale and robustness of cyberattacks has been increasing rapidly. Sensitive and confidential information are getting comprised across the network due to such attacks. To combat this threat, enterprises are taking mitigating actions to strengthen device access across their critical IT infrastructure.

Two-factor authentication significantly reduces the risk of adversaries penetrating strategic networks and systems. This approach requires the use of a Personal Identity Verification (PIV) card or Common Access Card (CAC). In this document, we will detail the basic procedures required to enable two-factor authentication for the Secure Shell Protocol (SSH) using government-issued PIV or CAC cards.



The authentication process is described below:

1. User starts SecureCRT client, enters the Cisco switch IP address in the hostname and press Enter.
2. A dialog box pops up prompting for PIN. User enters the PIN associated with the smartcard credential and press OK.



3. SecureCRT forwards certificate to Cisco Switch which validates Certificate handshake.
4. Cisco switch sends TACACS+ authorization request to IPS with username set to "common name" received from certificate and "service=pki"
5. IPS fetches the role and device group based on username and realm information.

6. If a shell policy has same role, device group with mandatory attribute set to "cert-application=all", then it is considered a match. If action is set to Permit, then IPS sends successful response containing all configured attributes.
7. User gets logged in to Cisco switch.

Pre-Requisites

- Cisco switch
- Ivanti Policy Secure Release 9.1R4 as TACACS+ Server
- SecureCRT (8.5.4) as the SSH client
- Smart Card Reader
- Common Access Card

Summary of Configuration

Configuring Ivanti Policy Secure

On IPS Server Administration UI, Admin configures:

- Admin Role
- Admin Realm
- TACACS Device group
- TACACS client
- Shell policy

To configure TACACS+ client and shell policy on IPS:

1. Select **Endpoint Policy > Network Device Management > TACACS+ client**, enable **Allow Authorization (w/o authentication)** under TACACS+ Advance Settings.

Network Device Administration > TACACS+ Client > New TACACS+ Client

New TACACS+ Client

▼ **TACACS+ Client**

* Name: Label to reference this TACACS+ Client.

Description:

* IP Address: IP Address of this TACACS+ Client.

* IP Address Range: Number of IP Addresses for this TACACS+ Client

* Shared Secret: TACACS+ shared secret

* Device Group: To manage groups, see the [Device Group](#)

▼ **TACACS+ Advance Settings**

Allow Authorization (w/o authentication) Allow Authorization (w/o authentication)

[Save Changes](#)

* Indicates required field

2. Select **Network Device Management > Shell Policies**.
3. Under **Custom attributes**, configure "*cert-application=all*" as mandatory attribute.
4. Click **Add**.
5. Click **Save Changes**.

Delete [X] [Y] [Z]

Command	Arguments	Action	
<input type="text"/>	<input type="text"/>	permit	Add

Deny any command that does not hit any of the rule in the table above

Permit any command that does not hit any of the rule in the table above

▼ **Custom Attributes**

Delete [X] [Y] [Z]

Attribute	Value	Requirement	
<input type="text"/>	<input type="text"/>	Mandatory	Add
cert-application	all	Mandatory	

▼ **Roles**

Policy applies to ALL roles

Policy applies to SELECTED roles

Policy applies to all roles OTHER THAN those selected below

Available roles:

Administrators

Read-Only Administrators

[Add](#) →

Selected roles:

tac_role

[Remove](#)

[Save Changes](#) [Cancel](#)

Cisco Switch Configuration

1. Set up Network Time Protocol (NTP) with the proper time zone for the device This step is critical for the operation of the public key infrastructure (PKI).

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
clock timezone EST -5 0
clock summer-time EDT recurring
ntp server <server ip>
```

2. Configure PKI trustpoint for the certificate authority (CA). Specify the field from the user certificate that will be used as the SSH username that will pass to the TACACS server for authorization. The example below uses the common name from the subnet field for the username. The user principal name (UPN) from the Subject-Alternative name can also be used as a username for SSH login.

```
crypto pki trustpoint <trustpoint name>
enrollment terminal
revocation-check none
authorization username subjectname commonname
```

3. Manually authenticate and install the root CA's public certificate.

```
crypto pki authenticate <trustpoint name>
```

4. Generate RSA signing and encryption keys for the SSH server.

```
crypto key generate rsa modulus 2048 label SSH-RSA usage-keys
```

5. Enable the SSH server and specify the RSA keys to be used for signing and encryption.

```
ip ssh rsa keypair-name SSH-RSA
ip ssh version 2
```


6. Configure the Cisco IOS SSH server to verify the user's X.509v3 digital credential for two-factor authentication.

```
ip ssh server certificate profile
  user
    trustpoint verify <trustpoint name>
    ip ssh server algorithm hostkey ssh-rsa
    ip ssh server algorithm authentication publickey
    ip ssh server algorithm publickey x509v3-ssh-rsa
```

7. Enable SSH for terminal line access, and enable X.509v3 validation.

```
aaa new-model
!
line vty 0 4
  login authentication default
  transport input ssh
```

8. Add the TACACS+ server and provision the shared secret and IP address of the TACACS+ server.

```
tacacs server IPS
  address ipv4 <server-ip>
  key <encryption key>
```

9. Configure TACACS+ for user authorization.

```
aaa group server tacacs+ IPS
  server name IPS
aaa authorization config-commands
aaa authorization exec IPS group tacacs+
aaa authorization commands 0 IPS group tacacs+ if-authenticated
aaa authorization commands 1 IPS group tacacs+ if-authenticated
aaa authorization commands 15 IPS group tacacs+ if-authenticated
aaa authorization network IPS group tacacs+
aaa authorization configuration IPS group tacacs+
```

10. Enable authorization on the PKI trustpoint CA for the user certificate.

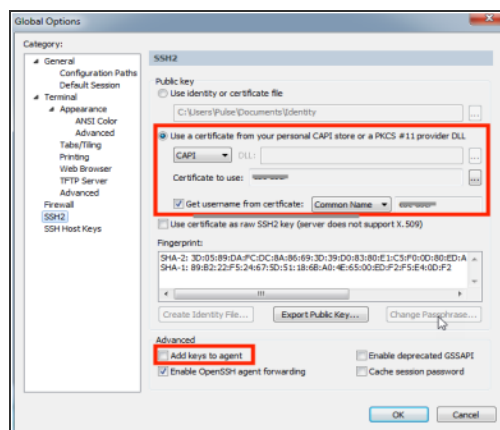
```
crypto pki trustpoint <trustpoint name>
  authorization list IPS
```

Configuring SecureCRT Client for Two-Factor Smartcard Authentication

If your SSH2 server environment is properly configured for X.509 smartcard certificate authentication, then you can configure SecureCRT/SecureFX to authenticate using Two-Factor Authentication certificates on your smartcard.

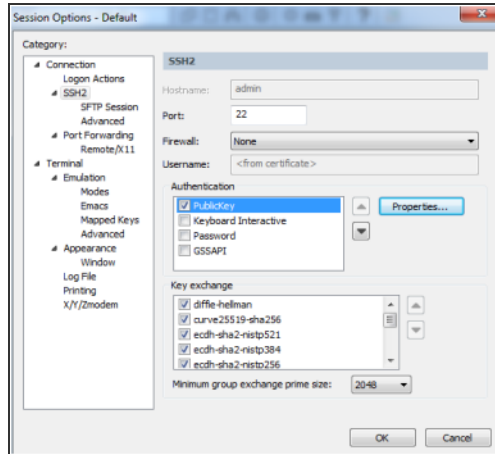
To configure SecureCRT/SecureFX for Windows to accomplish authentication using your smartcard:

1. Start the SecureCRT client. Open **Global Options** and select the **SSH2** category.
2. In the **Public key** section, enable **Use a certificate from your personal CAPI store or a PKCS #11 provider DLL** option.
3. Insert your smartcard.
4. For the **Certificate to use** field, press the [...] button to the right and browse through the available certificates.
5. If your certificate contains the user account name that should be used for authentication, enable the **Get username from certificate** option. Then specify the certificate field which contains the account name required for smartcard authentication to your SSH2 servers (either **Principal Name** or **Common Name**).
6. Disable the **Add keys to agent** option in the **Advanced** section below the fingerprint viewing area.

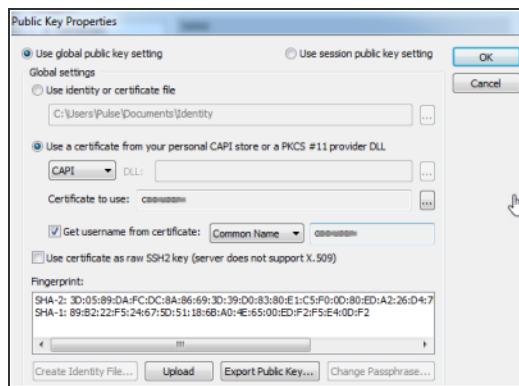


7. Click **OK** to save changes.
8. Choose **Options > Edit Default Session...**

9. Select the **SSH2** category. In the Authentication list, highlight the **PublicKey** authentication method and move it to the top of the list.
10. With **PublicKey** selected, press **Properties...** button.

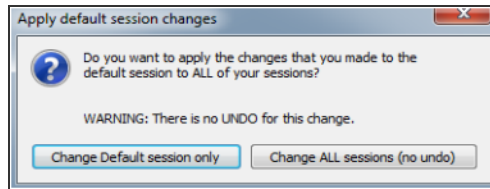


11. In the Public Key Properties window, enable the Use global public key setting option. Information should match what was specified in the Global Options settings above.



12. Press **OK** button to close the **Public Key Properties** window
13. Press **OK** button to close the **Session Options** window.

14. When prompted for selecting Apply default session changes, choose either of the option. If smartcard certificate will be authenticated for the majority of connections, then consider selecting Change ALL sessions (no undo).



As configured above, SecureCRT do not cache smartcard PIN. The first time user authenticate with a certificate on the smartcard, user will be prompted for the PIN by MS CAPI or your smartcard's middleware provider. If subsequently user is not prompted for PIN when authenticating with the smartcard, it is because PIN has been cached by smartcard's middleware.

Guest Access

Overview

Ivanti Policy Secure(IPS) provides guest access management solution through which you can manage and secure your guest network access.

Ivanti Policy Secure(IPS) supports the following mechanisms for guest access management:

- Guest Access through Guest User Account Manager (GUAM)
- Self-Registration
- Sponsor Approved Guest Access

Guest User Account Manager (GUAM)

The guest users use their own devices to access internet. A guest account can be created by a guest admin (GUAM) such as a receptionist. The GUAM user has below guest administration capabilities:

- Create temporary guest access accounts for guest users
- Create bulk accounts for numerous guest users
- Notify guest user credentials through email or text message.

Self-Registration

The guest self-registration enables a guest to access a Self-Registration URL and create their own guest account for internet access. The username and password for a self-provisioned guest account is delivered directly to the guest's web browser, or sent via SMS or email.

The self-registration workflow is described below:

1. The user connects to wireless network through guest SSID.
2. The user tries to access internet.
3. WLC redirects the user to IPS guest sign-in URL.

4. The user performs self-registration and signs-in through the credentials.
5. If the authentication is successful, the guest user can access internet.

Sponsor Approved Guest Access

The sponsor approved guest access provides access to the guest user only if it is approved by the Guest Sponsorer. The Sponsorer validates the guest user before giving the required access. This feature provides additional security by providing access only to valid guest users. The Sponsor takes the responsibility for the actions of the Guest and thus it brings accountability for the network usage and enhances the security of the network.

The sponsored guest access workflow is described below:

1. The Guest user connects to wireless network through guest SSID.
2. The Guest user performs the self-registration and the guest account will be created in disabled state and the access request is sent to the Sponsor (Employee/GUAM).
3. The Sponsorer will receive an email notification about the new guest access request.
4. The Sponsorer logs in to the Sponsor portal and approves/denies the guest user.
5. If the Sponsor approves the request the guest account becomes active and an email/SMS notification is sent to guest about activation of the account. If sponsor denies the request, the guest account will be deleted and an email/SMS notification is sent to guest about deny access.

Deployments

This topic describes the deployment scenarios of the Guest access solution.

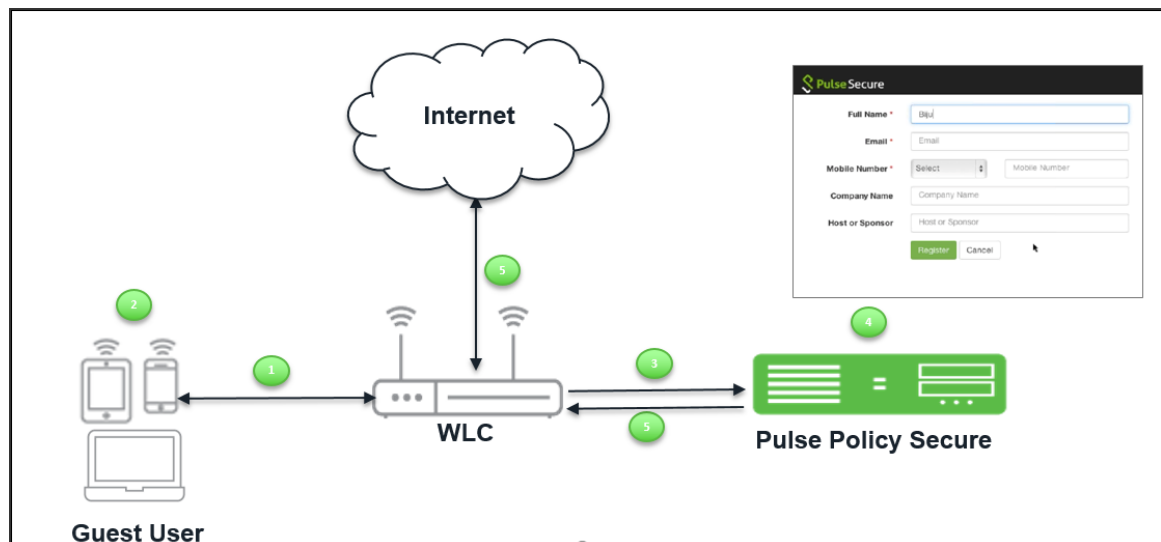
Guest Access using WLC

The guest access solution for wireless network can be deployed with leading Wireless LAN controllers. You can deploy wireless network with WLCs and wireless network for guests. The guest authentication is done with external authentication server and IPS server can be used as an external authentication server.

The assumption for this deployment the user has already deployed wireless network for guest using WLC and would like to have centralized authentication server. When wireless network is built with multiple vendors WLCs then it further becomes useful to have centralized authentication server.

The user flow is explained below:

1. Guest user comes on-premises and connects to guest SSID.
2. Guest user opens a browser to access an internet resource.
3. The user is redirected to IPS guest login page.
4. Guest user clicks the self-registration link from the guest login page and completes the registration process.
5. If the Administrator has configured Host Checker policy then IPS evaluates the Host Checker results.
6. Pre authentication – Host Checker policies are evaluated first and then user is prompted for credentials. For configuration details, see [User Realms](#)
7. Post authentication – User credentials are validated first and then the Host Checker policies are evaluated. For configuration details, see [User Roles](#)
8. Guest user logs in with guest user credentials. IPS validates the credentials and based on the result WLC redirects the guest user to the resource requested.



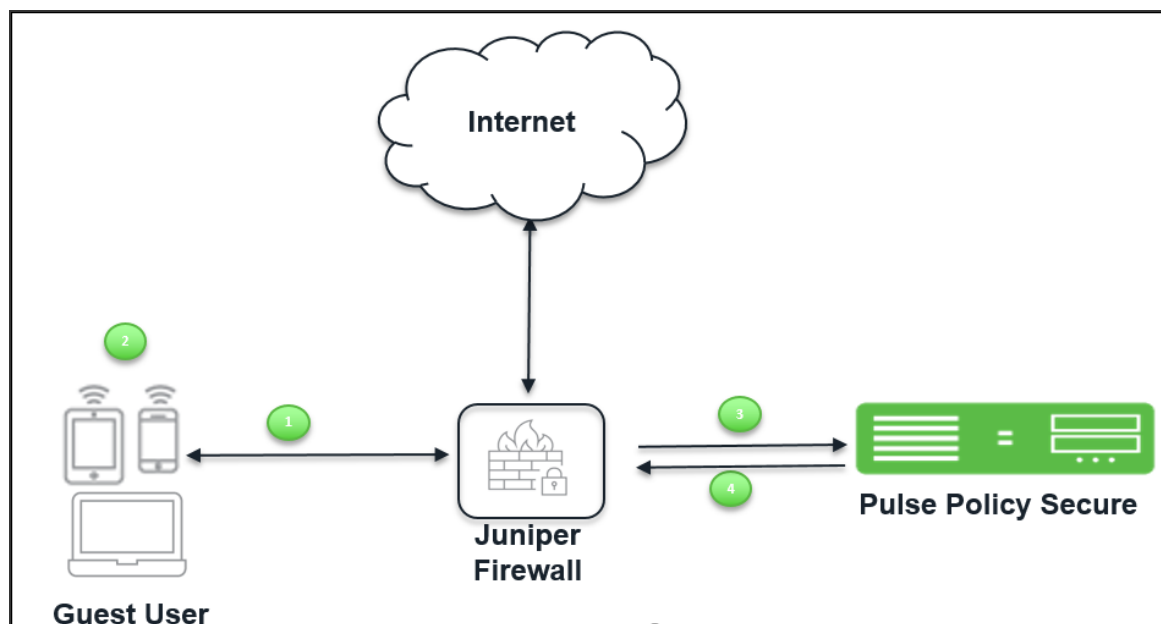
Guest Access using EX switch/SRX Firewall

When a IPS and an EX Series switch/SRX firewall is deployed, users must first sign into IPS for authentication before they can access a protected resource behind the EX Series switch/SRX firewall.

To facilitate sign-in, you can configure a redirect policy on the EX Series switch/SRX firewall to automatically redirect HTTP traffic destined for protected resources to IPS. When the sign-in page for the IPS is displayed, the user signs in, and access is granted to internet. These user accounts can be created by Guest User Account Manager.

The user flow is explained below:

1. Guest user comes on-premises and tries to connect to internet.
2. Guest user opens a browser to access an internet resource.
3. The Guest user is redirected to IPS login page.
4. If the Admin has configured Host Checker restrictions on the Guest role/realm then the Guest user is provided access only after Host Checker policies are evaluated.
5. The Admin can configure the Host Checker in two ways:
 6. **Pre-Authentication (Host Checker restriction on guest realm)**– The Host Checker policies are evaluated first and then user is prompted for credentials.
 7. **Post-Authentication (Host Checker restriction on guest role)** – The user credentials are validated first and then the host checker policies are evaluated.
8. The Guest user logs in with the credentials provided by the guest Admin (GUAM).

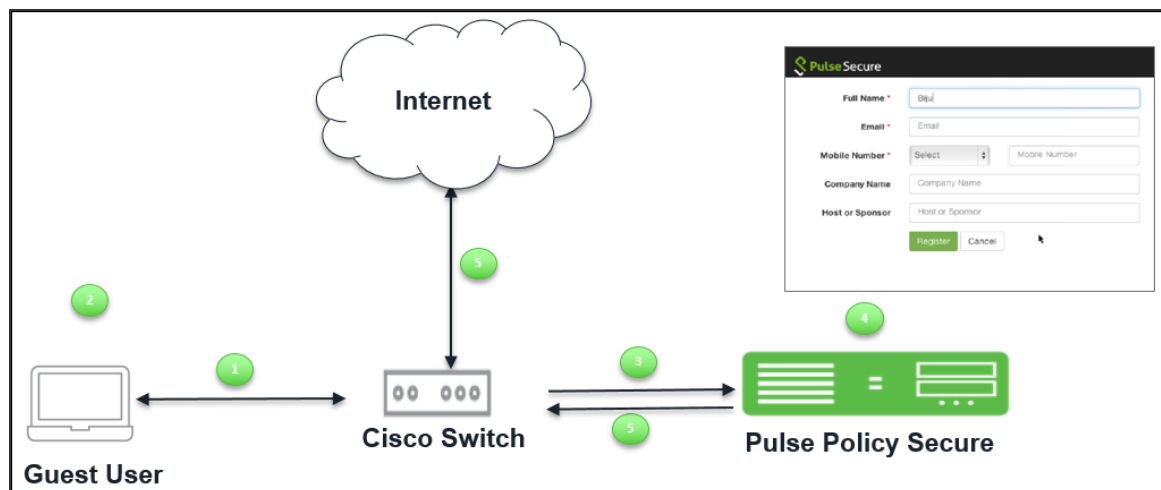


Guest Access using Cisco Switch

The guest access feature is supported for wired guest endpoints with Cisco switches. To facilitate sign-in, you can configure a redirect policy on the Cisco switch to automatically redirect HTTP traffic destined for protected resources through IPS . When the sign-in page for the IPS is displayed, the user signs in, and access is granted to internet.

The user flow is explained below:

1. Guest user comes on-premises and connects to LAN.
2. Guest user opens a browser to access an internet resource.
3. The user is redirected to IPS guest login page.
4. The Guest user self registers on IPS guest portal and receives the credentials over the email/SMS or on the UI.
5. If the Administrator has configured Host Checker policy then IPS evaluates the Host Checker results.
6. **Pre authentication** – Host Checker policies are evaluated first and then user is prompted for credentials. For configuration details, see User Realms.
7. **Post authentication** – User credentials are validated first and then the Host Checker policies are evaluated. For configuration details, see User Roles.
8. The guest user gets authenticated and gets redirected to the requested internet resource.



The configuration details are covered in [Configuring IPS for Guest Wired Authentication using Cisco Switch](#).

Configuring IPS for WLC Deployment

This section describes the configuration that is required on IPS to communicate with a Wireless LAN Controller (WLC) for Guest user management.

Ivanti Policy Secure(IPS) server acts as RADIUS server that allows to centralize the authentication and accounting for the users. You can add Cisco, Aruba, or Ruckus WLC as a RADIUS client on IPS. Guest user Self-Registration options need to be configured in the authentication server used for managing guest accounts and in sign-in policy settings.

Default Configurations for Guest Access

Ivanti Policy Secure(IPS) has some default configuration settings for convenience of the Admin users.

The default settings are:

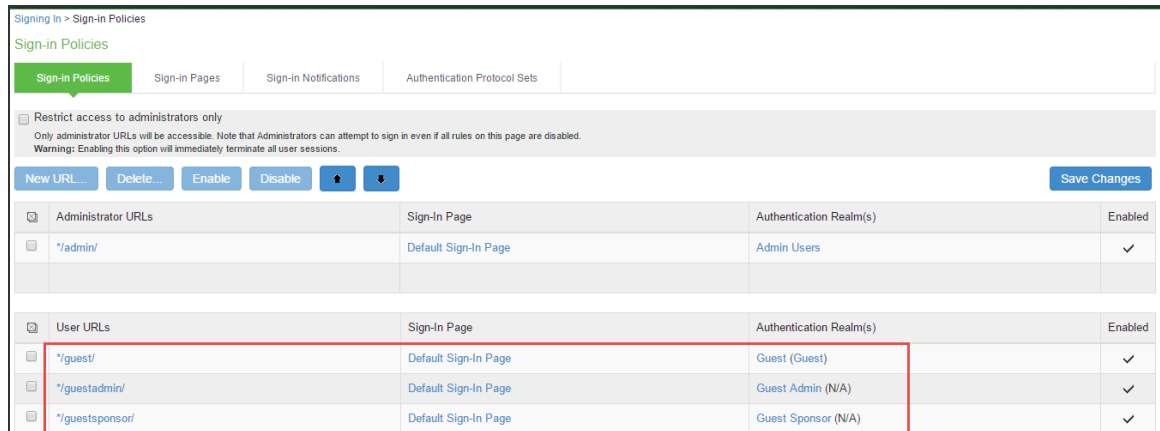
- Sign-in Policies
- User Realms
- User Roles
- Location Groups
- Authentication Protocol Sets
- Authentication Server

Sign-In-Policies

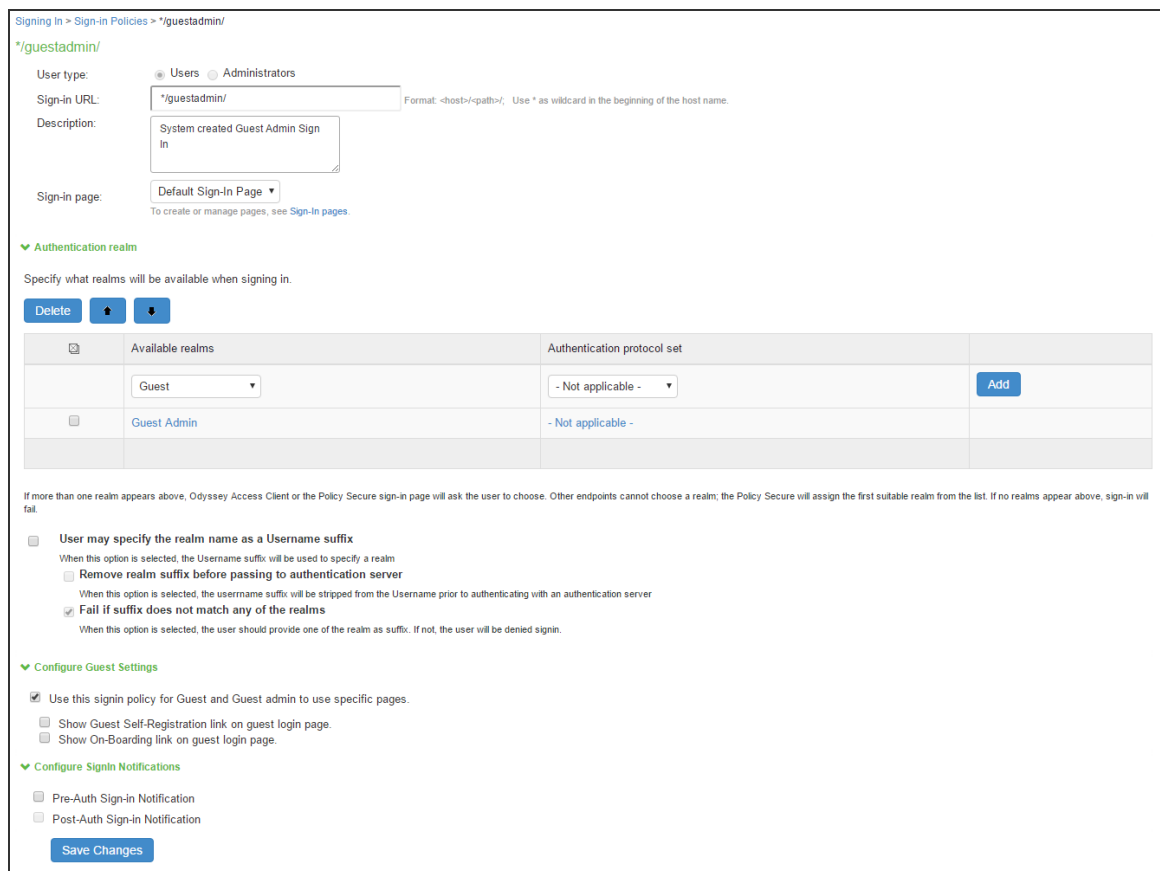
The */guestadmin/, */guest/, and */guestsponsor are the default Sign-in-Policies in IPS. A Sign-in Policy is mapped with a default Authentication Realm.

To view the Sign-in-Policies:

1. Select **Authentication > Signing In > Sign-in Policies**. The Sign-in Policies screen appears.



2. Click on a **Sign-in Policy** to view the settings. You can make necessary changes or add realms in a Sign-in Policy and click **Save Changes**.



User Realms

The Guest, Guest Admin and Guest Sponsor are the default user realms in IPS. A user realm is mapped with a default Role.



For a Guest Admin realm and Guest Sponsor Realm, Administrator must create the role mapping rule for the user name who has rights for creating Guest accounts.

To configure a guest admin realm:

1. Select **Users > User Realms**. The User Authentication Realms screen appears.

User Realms > User Authentication Realms

User Authentication Realms

View: Overview for all realms Update

New... Duplicate... Delete...

10 records per page Search:

Authentication Realm	Servers	Dynamic Policy Evaluation
<input type="checkbox"/> Cert Auth	Primary: Certificate Authentication	Disabled
<input type="checkbox"/> Guest	Primary: Guest Authentication	Disabled
<input type="checkbox"/> Guest Admin	Primary: Guest Authentication	Disabled
<input type="checkbox"/> Guest Sponsor	Primary: Guest Authentication	Disabled

2. Click on a **Guest Authentication Realm** to view the settings. The Role Mapping screen of the Realm appears.

User Realms > Guest > Role Mapping

Role Mapping

General Authentication Policy Role Mapping

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

New Rule... Duplicate Delete Up Down Save Changes

When users meet these conditions	assign these roles	Rule Name	Stop
1. username is "***"	→ Guest	rule 1	

When more than one role is assigned to a user:

- Merge settings for all assigned roles
- User must select from among assigned roles
- User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

3. Click an existing Rule of the Role to view the settings.

User Realms > Guest > Role Mapping > Role Mapping Rule

Role Mapping Rule

* Name:

▼ Rule:if username...

is If more than one username should match, enter one username per line. You can use * wildcards.

▼ then assign these roles

Available Roles:

Selected Roles:

Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

*Indicates required field

4. For Guest Sponsor, Click the **Guest Sponsor Realm** and specify how to assign the role. Click **New Rule** to add a new role and then click Save Changes.

User Realms > Guest Sponsor > Role Mapping > Role Mapping Rule

Role Mapping Rule

* Name:

▼ Rule:if username...

is If more than one username should match, enter one username per line. You can use * wildcards.

▼ then assign these roles

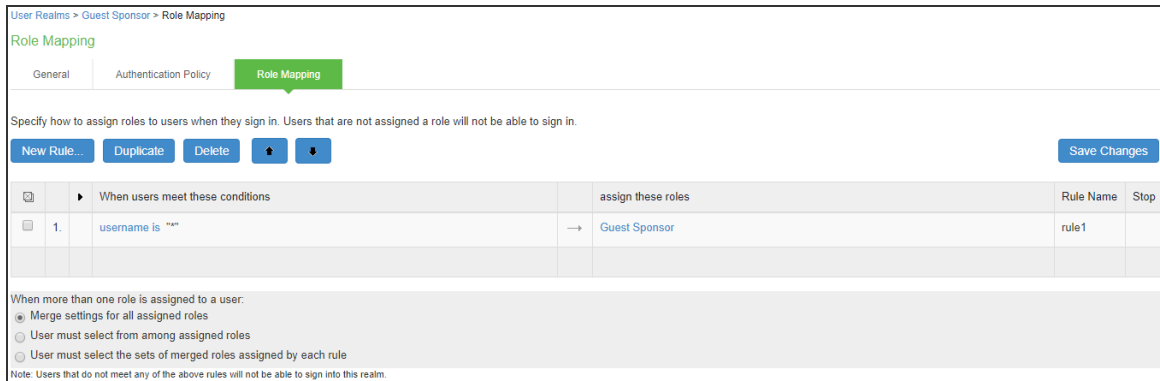
Available Roles:

Selected Roles:

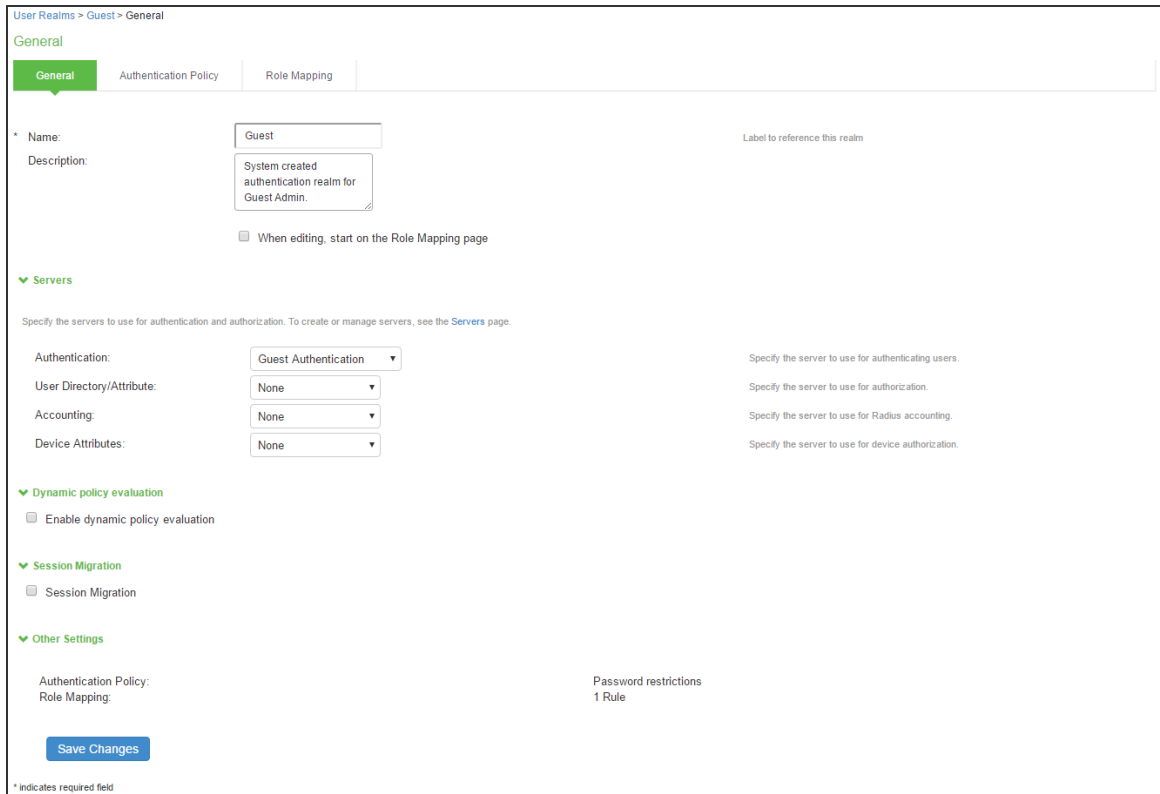
Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

- You can make necessary changes and click **Save Changes** to save the settings.



- Click the **General tab** to view the settings. The General screen appears.



- You can make necessary changes and click **Save Changes** to save the settings.

- Click **Host Checker**. You can make the necessary changes and click **Save Changes**.

The screenshot shows the 'Host Checker' configuration page. The breadcrumb trail is 'User Realms > Guest > Authentication Policy > Host Checker'. The page title is 'Host Checker'. There are three tabs: 'General', 'Authentication Policy' (which is active), and 'Role Mapping'. Below the tabs are several sub-sections: 'Source IP', 'Browser', 'Certificate', 'Password', 'Host Checker' (which is active), 'Limits', and 'RADIUS Request Policies'. A descriptive paragraph explains that users whose workstations meet the requirements specified by required host-checker policies will be allowed. Below this is a 'records per page' dropdown set to '10' and a search box. A table with three columns: 'Evaluate Policies', 'Require and Enforce', and 'Available Policies' is shown. The 'Available Policies' column contains the text 'All'. At the bottom of the table are navigation buttons: '← Previous', '1', and 'Next →'. Below the table is a checkbox labeled 'Allow access to realm if any ONE of the selected "Require and Enforce" policies is passed.' and a note: 'To manage Host Checker policies, see the Host Checker configuration page.' At the very bottom is a blue 'Save Changes' button.

User Roles

The Guest Admin, Guest, and Guest Sponsor are the default user roles in IPS. A user realm is mapped with a default Role.

To view a User Role:

- Select **Users > User Roles**. The Roles screen appears.

The screenshot shows the 'New Role' configuration page. The breadcrumb trail is 'User Roles > New Role'. The page title is 'New Role'. There are two input fields: 'Name:' with the value 'Full Access' and 'Description:' with an empty text area. Below these is a section titled 'Options' with a dropdown arrow. A note states: 'Session and appearance options are specified in Default Options. Check the following if this role should override these defaults.' There are five checkboxes: 'Session Options' (checked), 'UI Options' (checked), 'Odyssey Settings for Access' (unchecked), 'Odyssey Settings for Preconfigured Installer' (unchecked), 'Enable Guest User Account Management Rights' (unchecked), and 'Enable Sponsored Guest User Account Management Rights' (unchecked). At the bottom is a blue 'Save Changes' button.

- Click on a default Guest Role to view the settings.

- The **General > Overview** screen appears. You can make necessary changes and click **Save Changes** to save the settings.

Overview

General Agent Agentless

Overview Restrictions Session Options UI Options

Name: Users

Description: System created Users role.

Save Changes

Options

If these settings are not specified by any roles assigned to the user, the settings specified in Default Options will be used.

Session Options (Edit)

UI Options (Edit)

Enable Guest User Account Management Rights

Enable Sponsored Guest User Account Management Rights

Save Changes

- Click **Guest Sponsor** in the user role page to view the settings.

User Roles > Guest Sponsor > General > Overview

Overview

General Enterprise Onboarding Agent Agentless

Overview Restrictions Session Options UI Options

Name: Guest Sponsor

Description: System created Guest Sponsor role.

Save Changes

Options

If these settings are not specified by any roles assigned to the user, the settings specified in Default Options will be used.

Session Options (Edit)

UI Options (Edit)

Odyssey Settings for Policy Secure Access (Edit)

Odyssey Settings for Preconfigured Installer (Edit)

Enable Guest User Account Management Rights

Enable Sponsored Guest User Account Management Rights

Enterprise Device Onboarding

Save Changes

- You can go to other tabs of the User Roles, to view the default settings and make necessary changes.

Location Groups

The 'Guest' is the default Location Group configured in IPS. A Location Group is mapped with a default Sign-in Policy and a default Realm.

To view a Location Group:

1. Select **Endpoint Policy > Network Access > Location Group**. The Location Group screen appears.

Network Access > Location Group

Location Group

RADIUS Dictionary | RADIUS Vendor | **Location Group** | RADIUS Client | RADIUS Attributes | SNMP Device | SNMP Enforcement Policies

A location group policy logically groups network access devices by associating the devices with specific sign-in policies.

[New Location Group...](#) [Duplicate...](#) [Delete...](#)

10 records per page Search:

	Name	Sign-in Policy	MAC Auth Realm	RADIUS Clients
1	Default System created default location group	*/		
2	Guest System created location group for guest users	*/guest/		
3	Cert Auth System created location group for Certificate Authentication	*/certauth/		

2. Click the **Location Group** to view the settings.

Network Access > Location Group > Guest

Guest

Location Group

* Name: Label to reference this Location Group.

Description:

* Sign-in Policy: To manage policies, see the [Sign-In Policies](#)

MAC Authentication Realm: To manage realm, see the [MAC Address Realms](#)

[Save Changes](#)

* indicates required field

3. You can make necessary changes and click **Save Changes** to save the settings.

Authentication Protocol Set

The 'Guest' is the default Authentication Protocol Set configured in IPS.

To view the Authentication Protocol:

1. Select **Authentication > Signing In > Authentication Protocol Sets**. The Authentication Protocol screen appears.

Signing In > Authentication Protocols

Authentication Protocols

Sign-in Policies | Sign-in Pages | Sign-in Notifications | **Authentication Protocol Sets**

New Authentication Protocol... Duplicate... Delete... Restore Factory Default

10 records per page Search:

ID	Name	Authentication Protocol	PEAP	TTLS
1	802.1X System created default authentication protocol required for UAC agents	EAP-TTLS EAP-PEAP	EAP-JUAC EAP-MS-CHAP-V2	EAP-JUAC PAP MS-CHAP-V2 EAP-MS-CHAP-V2 EAP-GenericTokenCard
2	802.1X-Phones System created default authentication protocol for phones	EAP-MD5-Challenge EAP-TLS		
3	Guest System created authentication protocol for guest users	PAP CHAP		
4	Cert Auth System created authentication protocol for Certificate Authentication	EAP-TLS EAP-TTLS EAP-PEAP	EAP-JUAC EAP-TLS	EAP-JUAC EAP-GenericTokenCard

2. Click the **Authentication Protocol** to view the settings.

Signing In > Authentication Protocols > Guest

Guest

Name: Label to reference this Authentication Protocol.

Description:

▼ Authentication Protocol

Specify authentication protocols in preferred order

Available protocols: EAP-GenericTokenCard, EAP-MD5-Challenge, EAP-PEAP, EAP-TLS, EAP-TTLS

Add -> Remove

Selected protocols: PAP, CHAP

▼ PEAP

If EAP-PEAP is selected in authentication protocol and is not used for inner proxy, specify inner authentication protocols in preferred order

Available protocols: EAP-GenericTokenCard, EAP-JUAC, EAP-MS-CHAP-V2, EAP-SOH, EAP-TLS

Add -> Remove

Selected protocols: (none)

▼ TTLS

If EAP-TTLS is selected in authentication protocol and is not used for inner proxy, specify inner authentication protocols in preferred order

Available protocols: CHAP, EAP-GenericTokenCard, EAP-JUAC, EAP-MD5-Challenge, EAP-MS-CHAP-V2

Add -> Remove

Selected protocols: (none)

Save Changes

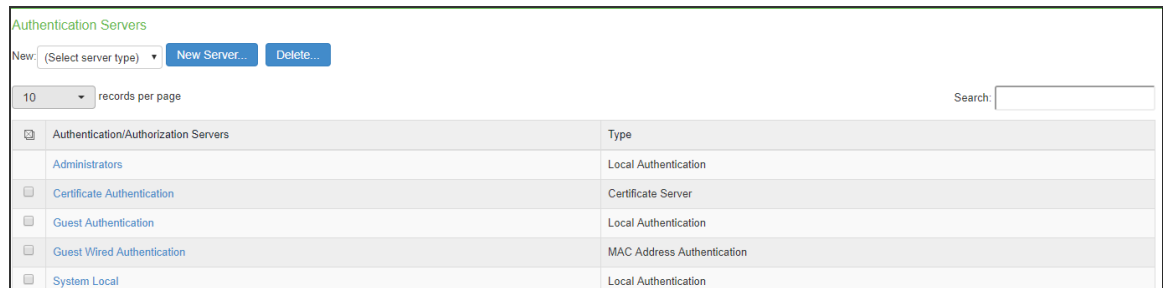
3. You can make necessary changes and click **Save Changes** to save the settings.

Authentication Server

The 'Guest Authentication and Guest Wired Authentication are the default Authentication Servers configured in IPS.

To view the Authentication Server:

1. Select **Authentication > Auth. Servers**. The Authentication Servers screen appears.



Authentication/Authorization Servers	Type
Administrators	Local Authentication
Certificate Authentication	Certificate Server
Guest Authentication	Local Authentication
Guest Wired Authentication	MAC Address Authentication
System Local	Local Authentication

2. Click the **Guest Authentication server** to view the settings.

3. The options under the Settings tab appears.

Auth Servers > Guest Authentication

Guest Authentication

Settings Users Admin Users

*Name: Label to reference this server.

▼ Password Options

Minimum length: characters
Maximum length: characters

Password must have at least digits
 Password must have at least letters
 Password must have mix of UPPERCASE and lowercase letters
 Password must be different from username
 New passwords must be different from previous password
 Password stored as clear text This option can only be set during create
Note: If password stored as clear text, more authentication protocols, i.e. CHAP, EAP-MD5, are supported

▼ Password Management

Allow users to change their passwords
 Force password change after days
 Prompt users to change their password days before current password expires

Note: Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities

▼ Guest Access

Guest User Account Managers

Enable Guest User Account Managers to administer Guest Accounts Configure system GUAM settings
Instructions for Guest User Account Manager:
Instructions displayed for guest users creation and updation. You can use ,
, , <noscript>, and <a href>-tags to format the text.

Maximum Account Validity Period: Set the Guest Account length limit (end time minus start time) in hours. This is valid for guests created by Guest Admin. Does not impact existing user expirations.

Guest Self-Registration

Send guest user credentials via: SMS
 Email Configure SMS/Email settings

Show credentials on screen after guest completes registration
 Enable Sponsored Guest Access

Response message for the Sponsor:
This message will be sent as email to the sponsor.

Approve message for the Guest:
This message will be sent as email/SMS to the guest user.

Deny message for the Guest:
This message will be sent as email/SMS to the guest user.

Maximum Account Validity Period for Self Registered Guests: Set the Guest Account length limit in hours. This is valid for self registered guests. Does not impact existing user expirations.

Note: To enable Guest Self-Registration navigate to Signing In > Sign-in Policies > User URLs > [url] > Configure Guest Settings

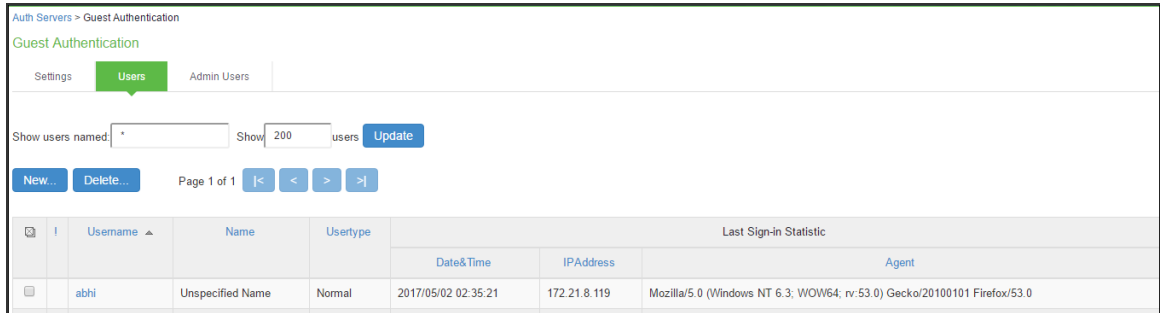
Common configuration for Guest User Account Managers and Guest Self-Registration

Guest User Name Prefix: Prefix applied to auto-generated user names.

Guest User Info Fields:
Enter additional fields for guest user information, one field per line. For example:
Title
Company name
Sponsor

* indicates required field

4. You can make necessary changes and click **Save Changes** to save the settings.
5. Click the Users tab to view the guest users list. This page displays all the users that are created by guest self-registration option, GUAM, and Sponsorer.



Configuring RADIUS Client on IPS

Ivanti Policy Secure(IPS) is configured with the default settings for RADIUS. You must configure only the RADIUS client and a RADIUS Return Attributes Policy.

To configure RADIUS Client on IPS:

1. Select **Endpoint Policy > Network Access > RADIUS Client > New RADIUS Client** to create a new RADIUS client. The New RADIUS Client screen appears.

The screenshot shows the configuration page for a new RADIUS client named 'Aruba'. The breadcrumb trail is 'Network Access > RADIUS Client > Aruba'. The page title is 'Aruba'. Under the 'RADIUS Client' section, the following fields are visible: Name (Aruba), Description (empty), IP Address (10.204.89.150), IP Address Range (1), Shared Secret (masked), Make/Model (Aruba Networks), and Location Group (Guest). To the right of these fields are labels: 'Label to reference this RADIUS Client', 'IP Address of this RADIUS Client', 'Number of IP Addresses for this RADIUS Client', 'RADIUS shared secret', 'To manage make/model, see the RADIUS Vendor', and 'To manage groups, see the Location Group'. Under the 'Dynamic Authorization Support' section, there are checkboxes for 'Support Disconnect Messages' (checked), 'Support CoA Messages' (checked), and 'Dynamic Authorization Port' (3799). There are also checkboxes for 'Disconnect Message Support', 'Change of Authorization Message Support', and 'Dynamic Authorization Extensions Port'. A 'Save Changes' button is at the bottom left, and a note '* indicates required field' is at the bottom.

The screenshot shows the configuration page for a new RADIUS client named 'Cisco'. The breadcrumb trail is 'Network Access > RADIUS Client > Aruba'. The page title is 'Aruba'. Under the 'RADIUS Client' section, the following fields are visible: Name (Cisco), Description (empty), IP Address (10.204.89.150), IP Address Range (1), Shared Secret (masked), Make/Model (Cisco Systems), and Location Group (Guest). To the right of these fields are labels: 'Label to reference this RADIUS Client', 'IP Address of this RADIUS Client', 'Number of IP Addresses for this RADIUS Client', 'RADIUS shared secret', 'To manage make/model, see the RADIUS Vendor', and 'To manage groups, see the Location Group'. Under the 'Dynamic Authorization Support' section, there are checkboxes for 'Support Disconnect Messages' (checked), 'Support CoA Messages' (checked), and 'Dynamic Authorization Port' (3799). There are also checkboxes for 'Disconnect Message Support', 'Change of Authorization Message Support', and 'Dynamic Authorization Extensions Port'. A 'Save Changes' button is at the bottom left, and a note '* indicates required field' is at the bottom.

The screenshot shows the configuration page for a new RADIUS client named 'Ruckus'. The breadcrumb trail is 'Network Access > RADIUS Client > New RADIUS Client'. The page title is 'New RADIUS Client'. Under the 'RADIUS Client' section, the following fields are visible: Name (Ruckus), Description (empty), IP Address (empty), IP Address Range (1), Shared Secret (masked), Make/Model (Ruckus Wireless), Ruckus Request Password (empty), Ruckus Server Certificate Validation (unchecked), and Location Group (Guest). To the right of these fields are labels: 'Label to reference this RADIUS Client', 'IP Address of the RADIUS Client', 'Number of IP Addresses for this RADIUS Client', 'RADIUS shared secret', 'To manage make/model, see the RADIUS Vendor', 'Ruckus SmartZone Northbound Portal Interface password (used for guest access)', 'Ruckus SmartZone Server Certificate Validation', and 'To manage groups, see the Location Group'. Under the 'Dynamic Authorization Support' section, there are checkboxes for 'Support Disconnect Messages' (unchecked), 'Support CoA Messages' (unchecked), 'Disconnect Message Support', and 'Change of Authorization Message Support'. A 'Save Changes' button is at the bottom left, and a note '* indicates required field' is at the bottom.

Configure the WLC (For example, Aruba, Cisco, Ruckus) as a RADIUS client and map with the default location group.



You can enable Ruckus Server Certificate Validation option to validate the device certificate. See [Verifying Device Certificates](#) for understanding the validation procedure.

2. Click **Save Changes** to save the settings.
3. Select **Endpoint Policy > Network Access > RADIUS Attributes > Return Attributes > New Policy** to create a new **RADIUS Return Attribute** policy.

Network Access > RADIUS Return Attributes Policies > New Policy

New Policy

* Name: Required: Label to reference this policy.

Description:

Location Group

Specify the Location Group for which this policy applies.

Available Location Groups:

Selected Location Groups: (all)

RADIUS Attributes

Open port

VLAN: (1 - 4094)

Return Attribute:

Return Attribute	Radius Auth Server Attribute Value	Auth Server Catalog Attribute Value	Value	
<input type="text" value="Ruckus-APN-NI"/>	<input type="text" value="-none-"/>	<input type="text" value="-none-"/>	<input type="text"/>	<input type="button" value="Add"/>

Add Session-Timeout attribute with value equal to the session lifetime

Add Termination-Action attribute with value equal 1

Interface

Specify the Interface which endpoints on this VLAN use to connect to the Pulse Policy Secure

Automatic (use configured VLANs)

Internal

External

Roles

Policy applies to ALL roles

Policy applies to SELECTED roles

Policy applies to all roles OTHER THAN those selected below

Available roles:

Selected roles: (none)

NOTE: changes to this page will cause all L2 clients to drop their connections and reconnect.

* indicates required field

- Map with the default location group. Configure other return attributes and session-timeout attributes as required.
- Click **Save Changes** to save the **Return Attribute Policy**.

Configuring SMTP and SMS gateway settings on IPS

The SMTP and SMS configuration settings must be configured to enable guest users to create user accounts on their own.

SMTP Settings for Guest User Accounts

To configure the SMTP settings:

- Select **System > Configuration > Guest Access > SMTP Settings**. The SMTP Settings screen appears.

The screenshot shows the 'SMTP Settings' configuration page. The breadcrumb trail is 'Configuration > Guest Access > SMTP Settings'. The page title is 'SMTP Settings'. The navigation menu includes 'Licensing', 'Pulse One', 'Security', 'Certificates', 'DMI Agent', 'Sensors', 'Client Types', 'SAML', 'Guest Access' (highlighted), 'Advanced Networking', and 'Notification'. Below the navigation, there are two tabs: 'SMTP Settings' (active) and 'SMS Gateway Settings'. The main content area is divided into two sections: 'General SMTP Settings' and 'Guest Access Settings'. In 'General SMTP Settings', there are fields for 'Email Account Details' (checkbox 'Enabled'), '*SMTP Server' (text input), 'SMTP Login' (text input), 'SMTP Password' (text input), '*SMTP Email' (text input), 'Use SSL' (checkbox 'Enabled'), and '*SMTP Port' (text input with '25'). In 'Guest Access Settings', there are fields for '*Email Subject' (text input) and '*Email Format' (radio buttons for 'html' and 'text'). A 'Save Changes' button is located at the bottom left.

2. Under General SMTP settings:
 - Enter the host name or IP address of the SMTP server.
 - Enter the SMTP login name.
 - Enter the SMTP password.
 - Enter the SMTP email address.
3. The Use SSL option supports the SMTP port 587.
4. Under Guest Access Settings:
 - Enter the email subject.
 - Select the email format- html, text.
5. Click **Save Changes**.

SMS Gateway Settings for Guest User Accounts

Short Message Service (SMS) is delivered through an SMS gateway service that supports HTTP, HTTPS, and SMTP (Simple Mail Transport Protocol) delivery. You need to subscribe to an external service to be able to deliver guest details using SMS. The SMS gateway sends SMS in formatted text message using HTTP/HTTPS interface (SMS message) and can also allow email message to be sent as an SMS. An example of an SMS gateway is clickatell.com. You should have a valid account with this third party.

To create an account with Clickatell:

1. Go to http://www.clickatell.com/products/sms_gateway.php, and choose the appropriate API sub-product (connection method) you wish to use.
2. Click on the registration hyperlink.
3. Select the Account type you would like to use (Local or International).
4. Enter your personal information to complete the registration form.
5. Accept the Terms & Conditions.
6. Click Continue - An email containing your log in details such as account log in name, password, and clientID will be sent to the email address you have provided.

7. Activate your account – When user has logged in, and user will be on the Clickatell Central landing page and HTTP API will be added to the account and client API ID will be issued to the account. A single account may have multiple API IDs associated with it.

Ivanti Policy Secure(IPS) integration with Clickatell

To enable the SMS gateway settings for Clickatell:

1. Select **System > Configuration > Guest Access > SMS Gateway Settings**. The SMS Gateway Settings screen appears.

The screenshot shows the 'SMS Gateway Settings' configuration page. At the top, there are tabs for 'SMTP Settings' and 'SMS Gateway Settings'. Below the tabs, there is a heading 'Enter settings to modify Guest User Account Manager and Guest Self-Registration features.' and a sub-heading 'The SMS gateway settings to send account details to guest via SMS.' A green arrow icon points to the 'SMS Gateway Settings' section.

The configuration fields include:

- Enable SMS Gateway Settings:**
- *SMS Gateway Type:** Clickatell API (dropdown menu)
- *SMS Gateway URL:** api.clickatell.com
- *API product ID:** 1234 (text input)
- *SMS Gateway Login Name:** (text input)
- *SMS Gateway Password:** (text input)
- Source Mobile Number:** Select (dropdown menu)
- HTTPS:** Secure Channel.
- Use Proxy Server:**
 - Address:** (text input)
 - Port:** 80
 - Username:** (text input)
 - Password:** (text input)
- Text Message(SMS) Format(Optional Fields):**
 - Guest Account Start Time
 - Guest Account End Time
 - Guest Account Sign-In URL: 10.204.90.17/gue
 - Wireless SSID: openedu

A blue 'Save Changes' button is located at the bottom right of the form.

2. Select the **Enable SMS Gateway Settings** check box.
3. Complete the configuration settings as described in table.
4. Click **Save Changes**.
5. Select the **Country** and enter the mobile number. Click **Send Test SMS**.

Settings	Guidelines
SMS Gateway Settings	
SMS Gateway Type	<p>Select the gateway type:</p> <p>Clickatell Platform- Select this option to send SMS as a text message. Use "Clickatell Platform" for accounts that use "platform.clickatell.com" as gateway.</p> <p>Clickatell API- Select this option to send SMS as a text message. Use "Clickatell API" for accounts that use "api.clickatell.com" as gateway.</p> <p>Clickatell Email2SMS – Select this option to use email format as an SMS using SMTP.</p>
API product ID	Specify the API product ID that you received from Clickatell during account creation.
SMS Gateway Login Name	Specify the SMS gateway login name.
SMS Gateway Login password	Specify the SMS gateway login password.
Text Message (SMS) Format	<p>(Optional) Select the following fields:</p> <p>Guest Account Start Time</p> <p>Guest Account End Time</p> <p>Guest Account Sign-in URL</p> <p>Wireless SSID</p>
The following options apply if you select Clickatell Platform as gateway type.	
SMS Gateway URL	Specify the SMS Gateway URL. (Default) https://api.clickatell.com or http://api.clickatell.com
HTTPS	Select this option to use a secure connection. If you don't select this option user will be notified about clear text transmission of guest user credentials.
Use Proxy Server	Select this option to access the internet or SMS gateway URL using a proxy server.
Address	Specify the address of the proxy server and its port.
Username	Specify the username of the proxy server.

Settings	Guidelines
Password	Specify the password of the proxy server.
Send Test SMS	
Mobile Number	Select the country name and then specify a valid phone number of the guest user. The phone number should not include country code or any special character such as +, *, and so on. The IPS sends a test SMS with the login credentials to this mobile number through SMS.
Source Mobile Number	Specify the sender ID configured in Clickatell Account

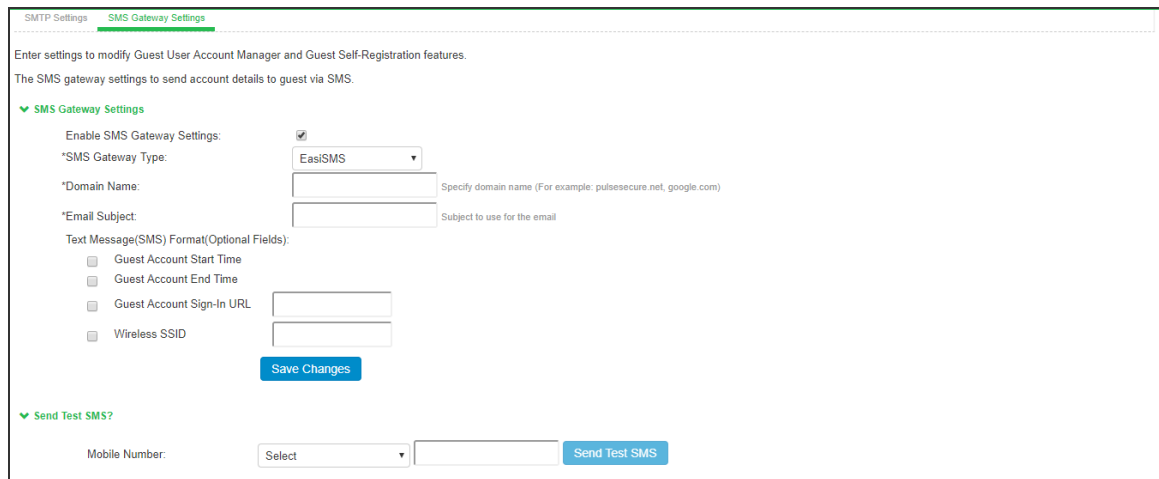
Ivanti Policy Secure(IPS) integration with EasiSMS

Ivanti Policy Secure(IPS) integrates with EasiSMS through the SMTP server. EasiSMS uses an email format to send SMS to end user mobile phones.

 Ensure SMTP server is configured to use the EasiSMS feature.

To configure the SMS gateway settings for EasiSMS on IPS:

1. Select **System > Configuration > Guest Access > SMS Gateway Settings**.
2. The SMS Gateway Settings screen appears.



The screenshot shows the 'SMS Gateway Settings' configuration page. At the top, there are tabs for 'SMTP Settings' and 'SMS Gateway Settings'. Below the tabs, there is a heading: 'Enter settings to modify Guest User Account Manager and Guest Self-Registration features. The SMS gateway settings to send account details to guest via SMS.' The main configuration area is titled 'SMS Gateway Settings' and includes the following fields and options:

- Enable SMS Gateway Settings:** A checked checkbox.
- *SMS Gateway Type:** A dropdown menu with 'EasiSMS' selected.
- *Domain Name:** An empty text input field with a placeholder note: 'Specify domain name (For example: pulsesecure.net, google.com)'.
- *Email Subject:** An empty text input field with a placeholder note: 'Subject to use for the email'.
- Text Message(SMS) Format(Optional Fields):** A section with four unchecked checkboxes:
 - Guest Account Start Time
 - Guest Account End Time
 - Guest Account Sign-In URL
 - Wireless SSID
- Save Changes:** A blue button.
- Send Test SMS?:** A section with a 'Mobile Number:' label, a 'Select' dropdown menu, an empty text input field, and a 'Send Test SMS' button.

3. Select Enable SMS Gateway Settings check box.
4. Select the SMS Gateway Type as EasiSMS.
5. Enter the Domain Name provided by EasiSMS.
6. Enter the unique ID in Email Subject provided by EasiSMS.
7. Optionally configure Text Message Format.
8. Click **Save Changes**.

When a guest user registers on the guest portal, the user receives an SMS with the login credentials that allows the user to access the resources.

Configuring Guest Access Settings on IPS

To configure guest access settings on IPS:

1. Select **Authentication > Auth. Servers > System Local > Settings**.
2. Under Guest Access Configurations:
 - Select the check box **Enable Guest User Account Managers** to administer Guest Accounts.
 - Under the Guest Self-Registration select Send guest user credentials via
 - SMS
 - Email
 - Click the SMS/Email settings link and do the necessary settings.
 - Show credentials on screen after guest completes registration
 - Maximum Account Validity Period for Self Registered Guest – Default is 24 hours. You can change this as per the requirement.
 - For Sponsored Guest Access, select Enable Sponsored Guest Access.



Self-Registration is supported only with WLC deployment.

Guest Self-Registration
Send guest user credentials via: SMS Email [configure SMS/Email settings](#)

Show credentials on screen after guest completes registration

Enable Sponsored Guest Access

Response message for the Sponsor: This message will be sent as email to the sponsor.

Approve message for the Guest: This message will be sent as email/SMS to the guest user.

Deny message for the Guest: This message will be sent as email/SMS to the guest user.

Maximum Account Validity Period for Self Registered Guests: Set the Guest Account length limit in hours. This is valid for self registered guests. Does not impact existing user expirations.

Note: To enable Guest Self-Registration navigate to Signing In > Sign-in Policies > User URLs > [url] > Configure Guest Settings

3. Select **Authentication > Signing In > Sign-In Policies**.

New Sign-In Policy

User type: Users Administrators

Sign-in URL: Format: <host>/<path>/ Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: To create or manage pages, see [Sign-In pages](#).

Authentication realm

Specify how to select an authentication realm when signing in.

User types the realm name
The user must type the name of one of the available authentication realms.

User picks from a list of authentication realms
The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or manage realms, see the [Administrator Authentication page](#).

Available realms:

Selected realms:

Configure Signin Notifications

Pre-Auth Sign-in Notification

Post-Auth Sign-in Notification

4. Select the sign-in policy that is created earlier.

Under Configure Guest settings select the check boxes:

- Use this sign-in policy for Guest and Guest admin to use specific pages
- Show Guest Self Registration link on the guest log in page.

5. The Register as Guest link appears on the guest log in page.

Configuring IPS for SRX/EX Deployment

The Administrator must follow the below procedure for enabling guest access using SRX firewall:

- Default Configurations for Guest Access
- Configuring SMTP and SMS Gateway
- Configuring Guest Access Settings on IPS.

To configure captive portal:

1. From IPS admin UI, select **Endpoint Policy > Infranet Enforcer > Connection** and add **SRX/EX**.

infranet Enforcer > Connection > New Infranet Enforcer

New Infranet Enforcer

▼ Infranet Enforcer

Platform: JUNOS SRX Platform of this Infranet Enforcer.

* Name: Label to reference this Infranet Enforcer.

* Password: Connection password.

* Serial number(s): One per line.

Location Group: Guest To manage groups, see the Location Group

▼ Coordinated Threat Control

Note that not all enforcer versions and platforms have an IDP module.

Use IDP Module as Sensor

Save Changes

2. From the SRX CLI configuration menu, configure a captive portal named guests that redirects the unauthenticated traffic to guest URL. For example <https://xyz.abc.local/guest>.
3. Create a new policy that redirects any source that attempts to access the server.
4. You can also create Host Checker restrictions on the Guest realm/role.

Configuring IPS for Guest Wired Authentication using Cisco Switch

This section describes the configuration that is required on IPS to communicate with a Cisco switch for Guest wired authentication.

To configure IPS for guest wired authentication:

1. Select **Authentication > Auth. Servers**. The Authentication Servers screen appears.

Authentication Servers

New: (Select server type) New Server... Delete...

10 records per page Search:

Authentication/Authorization Servers	Type
Administrators	Local Authentication
Certificate Authentication	Certificate Server
Guest Authentication	Local Authentication
Guest Wired Authentication	MAC Address Authentication
System Local	Local Authentication

2. Click **Guest Wired Authentication** available by default to view the settings.

Auth Servers > Guest Wired Authentication > Settings

Settings

Name: Label to reference this authentication.

MAC Addresses

Maximum 500 addresses

Delete

MAC Address	Action	Attributes	
<input type="text"/>	Allow	<input type="text"/>	<input type="button" value="Add"/>
*****	Allow		

Example MAC Address:
00:11:85:bb:8c:66
00:#+--+
Example Attribute:
attribute1=value1,attribute2=value2,
(for attribute: alphanumeric or '_' or '-' characters only)
The Allow & Attributes action accepts the defined MAC Address expression and looks it up in the optional LDAP Server(s) below for authorization attributes.

Optional LDAP Servers

Available LDAP Servers: (none)

Selected LDAP Servers: (none)

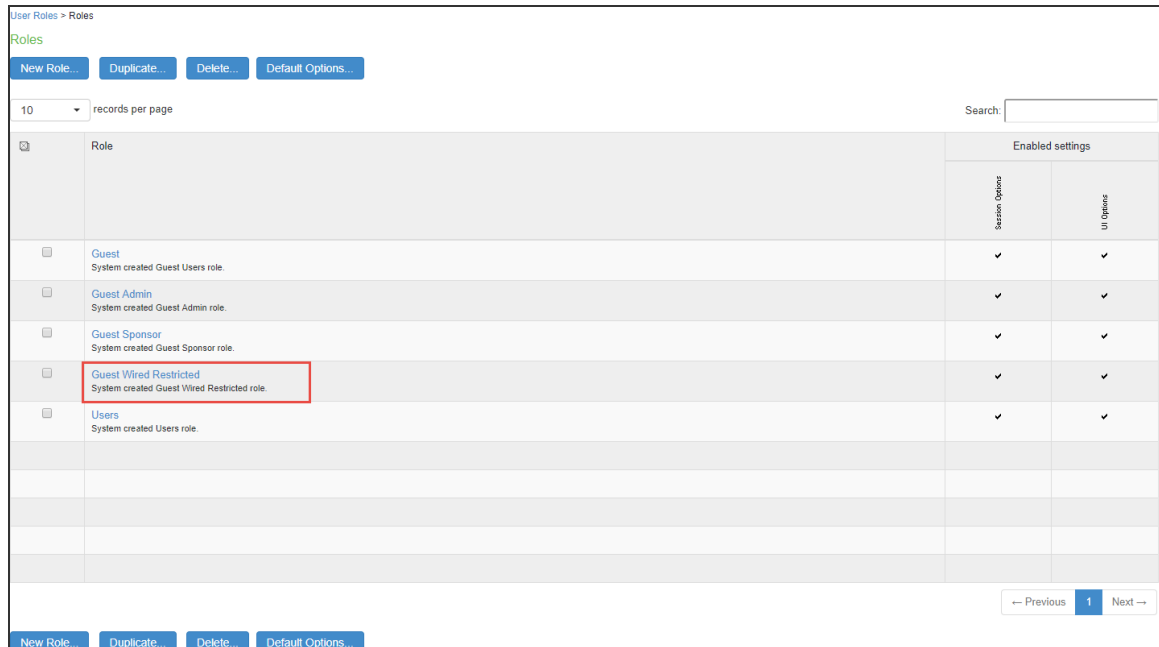
To manage servers, see the [Server configuration page](#).

Server Catalog

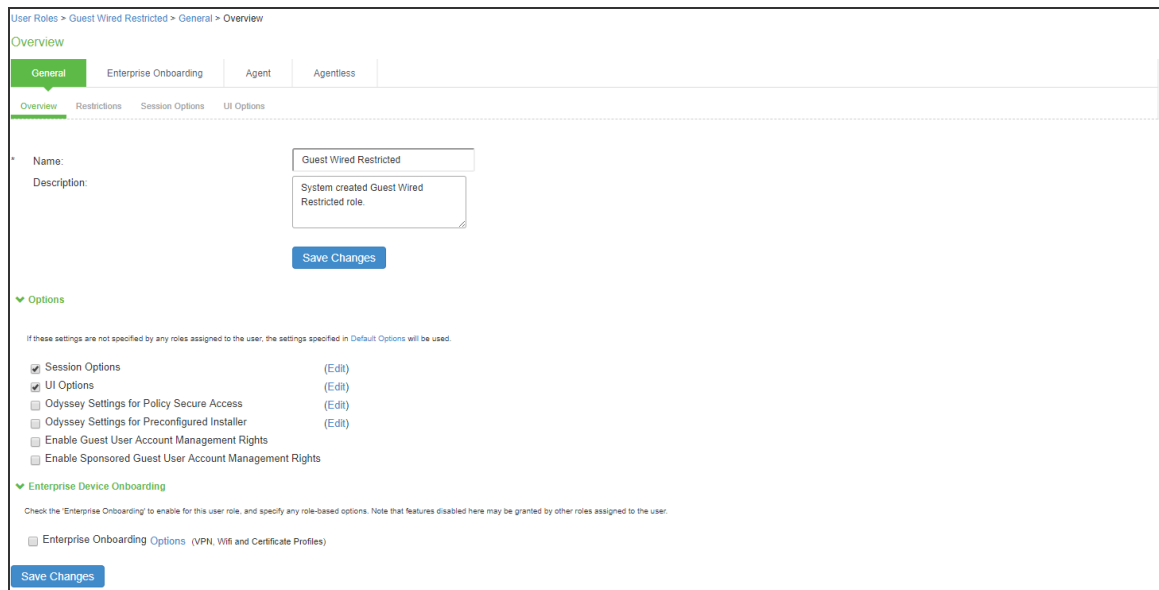
The attributes catalog should be used for both attributes defined in the MAC Addresses Table and the optional LDAP Servers.

3. You can make the necessary changes and click **Save Changes**.

4. Select **Users > User Roles**. The User Roles page appears.



5. Click **Guest Wired Restricted** user role available by default. The Agentless access is enabled for this role. You can also configure Host Checker for assessing the compliance status of the endpoint.



- Select **Endpoint Policy > MAC Address Authentication Realms** and click **Guest Wired authentication** realm available by default.

MAC Address Realms > Guest Wired > General

General

General Authentication Policy Role Mapping

Name: Guest Wired Label to reference this realm

Description: System created MAC authentication realm for Guest Wired users.

When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Guest Wired Authentication Specify the server to use for authenticating users.

User Directory/Attribute: Same as above Specify the server to use for authorization.

Accounting: None Specify the server to use for Radius accounting.

Device Attributes: None Specify the server to use for device authorization.

Dynamic policy evaluation

Enable dynamic policy evaluation

Other Settings

Authentication Policy: Password restrictions
Role Mapping: 1 Rule

Save Changes

- Select the default role mapping rule, which specifies the conditions to assign the Guest Wired Restricted role.

MAC Address Realms > Guest Wired > Role Mapping

Role Mapping

General Authentication Policy Role Mapping

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

New Rule... Duplicate Delete ↑ ↓ Save Changes

	When users meet these conditions	assign these roles	Rule Name	Stop
1.	username is *	→ Guest Wired Restricted	rule 1	

When more than one role is assigned to a user the settings for all assigned roles will be merged.
Note: Users that do not meet any of the above rules will not be able to sign into this realm.

8. Select **Endpoint Policy > Network Access > Location Group**. Select **Guest Wired** as MAC Auth Realm.

Network Access > Location Group > Guest Wired

Guest Wired

▼ Location Group

* Name: Label to reference this Location Group

Description:

* Sign-in Policy: To manage policies, see the [Sign-In Policies](#)

MAC Authentication Realm: To manage realm, see the [MAC Address Realms](#)

9. Configure the Cisco switch as a RADIUS client. Ensure that the Guest Wired location group and Support CoA Messages options are enabled.

Network Access > RADIUS Client > Cisco wired

Cisco wired

▼ RADIUS Client

* Name: Label to reference this RADIUS Client

Description:

* IP Address: IP Address of this RADIUS Client

* IP Address Range: Number of IP Addresses for this RADIUS Client

* Shared Secret: RADIUS shared secret

* Make/Model: To manage make/model, see the [RADIUS Vendor](#)

Location Group: To manage groups, see the [Location Group](#)

▼ Dynamic Authorization Support

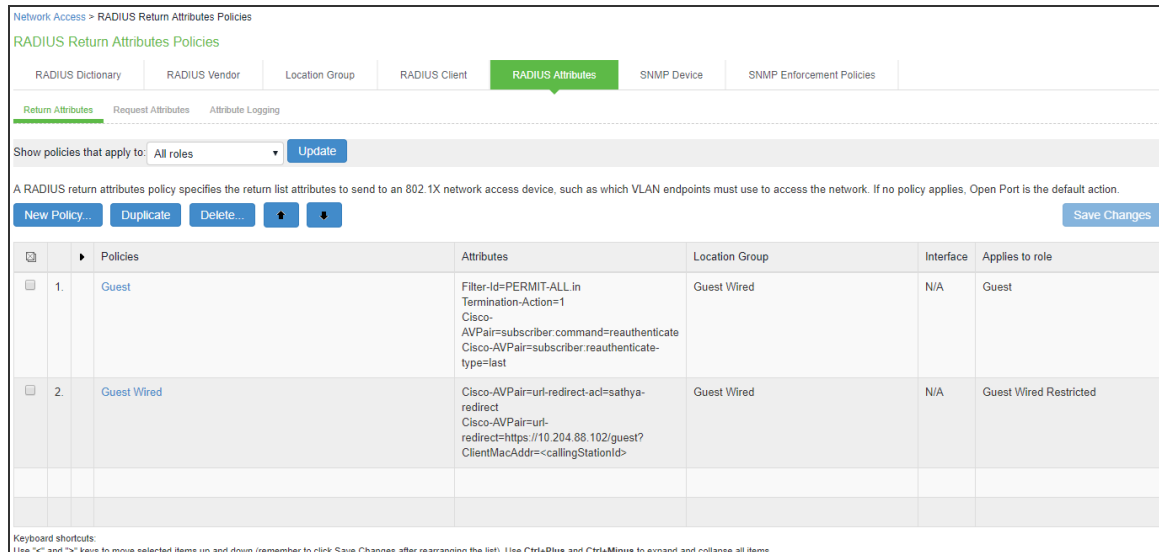
Support Disconnect Messages Disconnect Message Support

Support CoA Messages Change of Authorization Message Support

* Dynamic Authorization Port: Dynamic Authorization Extensions Port

* indicates required field

- Configure the RADIUS return attributes for Guest Wired policy. The RADIUS return attributes are required for moving the endpoint to the appropriate VLAN.



- The user configures the RADIUS URL-redirection attributes on the Cisco Switch. Using RADIUS URL-Redirection return attributes the Cisco switch redirects any initial HTTP/s traffic to IPS.

You must configure the following return attributes (supported only on Cisco switches):

```
Cisco-AVPAIR=url-redirect-acl=REDIRECT_To_IPS
Cisco-AVPAIR=url-redirect=https://<IPS-SIGN-IN-URL>/guest?ClientMacAddr=<callingStationId>
```

Here in redirect guest portal URL (* /guest), the "ClientMacAddr" is to identify the end client being redirected to IPS. As part of MAB authentication, IPS updates the value of radius return attribute "url-redirect" and replaces <callingStationId> with the client MAC address.

The RADIUS CoA configuration for various Cisco switch platforms is described below.

Cisco Platform	IOS Version	RADIUS CoA Configuration
3850	16.3	Filter-Id=PERMIT-ALL.in
2960X	15.2	Filter-Id=PERMIT-ALL.in

Cisco Platform	IOS Version	RADIUS CoA Configuration
2960	12.2	Filter-Id=PERMIT-ALL.in CiscoAVPAIR=subscriber:command=reauthenticate Cisco-AVPAIR=subscriber:reauthenticate- type=last

Network Access > RADIUS Return Attributes Policies > Guest Wired

Guest Wired

General

* Name: Required. Label to reference this policy.

Description:

Location Group

Specify the Location Group for which this policy applies.

Available Location Groups:

Selected Location Groups:

RADIUS Attributes

Open port

VLAN:

Return Attribute:

<input type="checkbox"/>	Return Attribute	Radius Auth Server Attribute Value	Auth Server Catalog Attribute Value	Value	
<input type="checkbox"/>	<input type="text" value="Filter-Id"/>	<input type="text" value="-none-"/>	<input type="text" value="-none-"/>	<input type="text"/>	<input type="button" value="Add"/>
<input type="checkbox"/>	Cisco-AVPair	-none-	-none-	url-redirect-act=sathya-redirect	
<input type="checkbox"/>	Cisco-AVPair	-none-	-none-	url-redirect=https://10.204.88.102/guest?ClientMacAddr=<callingStationId>	

Add Session-Timeout attribute with value equal to the session lifetime

Add Termination-Action attribute with value equal 1

Interface

Specify the Interface which endpoints on this VLAN use to connect to the Pulse Policy Secure

Automatic (use configured VLANs)

Internal

External

Roles

Policy applies to ALL roles

Policy applies to SELECTED roles

Policy applies to all roles OTHER THAN those selected below

Available roles:

Selected roles:

NOTE: changes to this page will cause all L2 clients to drop their connections and reconnect.

Configuring IPS for Sponsored Guest Access

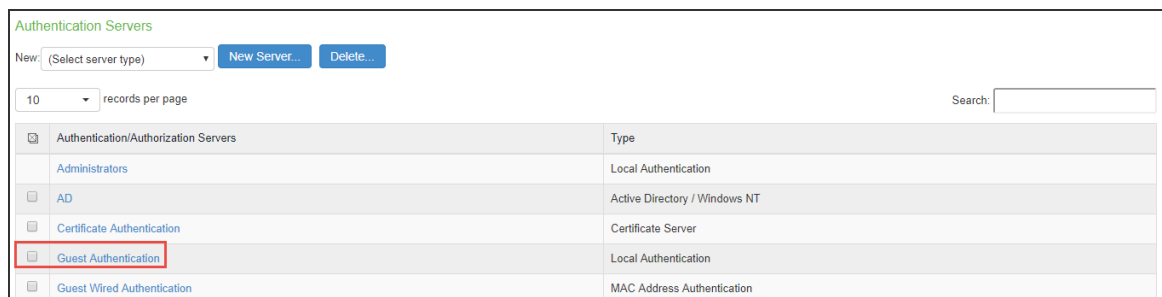
This section describes the configuration that is required for configuring Sponsored Guest access.

- Enable "Sponsored Guest Access" checkbox under Guest Authentication Server.
- Create a list of Sponsor's names in Guest Authentication Server.

- Create Role mapping rule in "Guest Admin" realm to point to "Sponsor" role for the list of sponsor's.
- If sponsor reside in AD, then AD needs to be selected as authentication server instead of "Guest Authentication" under "Guest Admin" realm.
- As part of default configuration, "sponsor" role is created with enabled sponsor management rights. This role can be used for sponsor approved guest access.

To configure IPS for Sponsored Guest access:

1. Select **Authentication > Auth. Servers**. The Authentication Servers screen appears. Click **Guest Authentication** available by default to view the settings.



2. Select **Enable Sponsored Guest Access**.



3. Select **Email to send guest user credentials through email**. You can make the necessary changes and click **Save Changes**.

Auth Servers > Guest Authentication > Settings

Settings

*Name: Guest Authentication Label to reference this server.

[Password Options](#)
[Password Management](#)
[Guest Access](#)

Guest User Account Managers

Enable Guest User Account Managers to administer Guest Accounts Configure system GUAM settings

Instructions for Guest User Account Manager:

Instructions displayed for guest users creation and updation. You can use ,
, , <noscript>, and <a href= tags to format the text.

Maximum Account Validity Period: 24 Set the Guest Account length limit (end time minus start time) in hours. This is valid for guests created by Guest Admin. Does not impact existing user expirations.

Guest Self-Registration

Send guest user credentials via: SMS Email Configure SMS/Email settings

Show credentials on screen after guest completes registration

Enable Sponsored Guest Access

Maximum Account Validity Period for Self Registered Guests: 24 Set the Guest Account length limit in hours. This is valid for self registered guests. Does not impact existing user expirations.

Note: To enable Guest Self-Registration navigate to Signing In > Sign-in Policies > User URLs > [url] > Configure Guest Settings

Common configuration for Guest User Account Managers and Guest Self-Registration

Guest User Name Prefix: guest_ Prefix applied to auto-generated user names.

Guest User Info Fields:

Enter additional fields for guest user information, one field per line. For example:

Company Name
Host or Sponsor
Title
Company name
Sponsor

4. Select **Users > User Roles**. The User Roles page appears.

10 records per page Search:

Role	Enabled settings							
	Session Options	UI Options	UAC Agent	Host Enforcer	IC Access	Preconfig	Agentless Access	Outboard
<input type="checkbox"/> Guest <small>System created Guest Users role.</small>	✓	✓					✓	
<input type="checkbox"/> Guest Admin <small>System created Guest Admin role.</small>	✓	✓					✓	
<input checked="" type="checkbox"/> Guest Sponsor <small>System created Guest Sponsor role.</small>	✓	✓					✓	
<input type="checkbox"/> Guest Wired Restricted <small>System created Guest Wired Restricted role.</small>	✓	✓					✓	

- Click **Guest Sponsor user role** available by default. Select **Enable Sponsored Guest User Account Manager Rights**.

User Roles > Guest Sponsor > General > Overview

Overview

General Enterprise Onboarding Agent Agentless

Overview Restrictions Session Options UI Options

* Name: Guest Sponsor

Description: System created Guest Sponsor role.

Save Changes

Options

If these settings are not specified by any roles assigned to the user, the settings specified in Default Options will be used.

- Session Options (Edit)
- UI Options (Edit)
- Odyssey Settings for Policy Secure Access (Edit)
- Odyssey Settings for Preconfigured Installer (Edit)
- Enable Guest User Account Management Rights
- Enable Sponsored Guest User Account Management Rights**

- Once you configure Sponsor Guest Access. You can see the Sponsor email entry in the Guest Self registration page.

Full Name * Full Name

Email Email

Mobile Number Select Mobile Number

Company Name Company Name

Host or Sponsor Host or Sponsor

Sponsor Email * Email

Register Cancel

- Select **Authentication > Signing In > Sign-in Policies** and use the default `*/guestsponsor/` sign-in policy.

8. Select **Users > User Realms**. Click the **Guest Sponsor Realm** and specify how to assign the role. Click **New Rule** to add a new role and then click **Save Changes**.

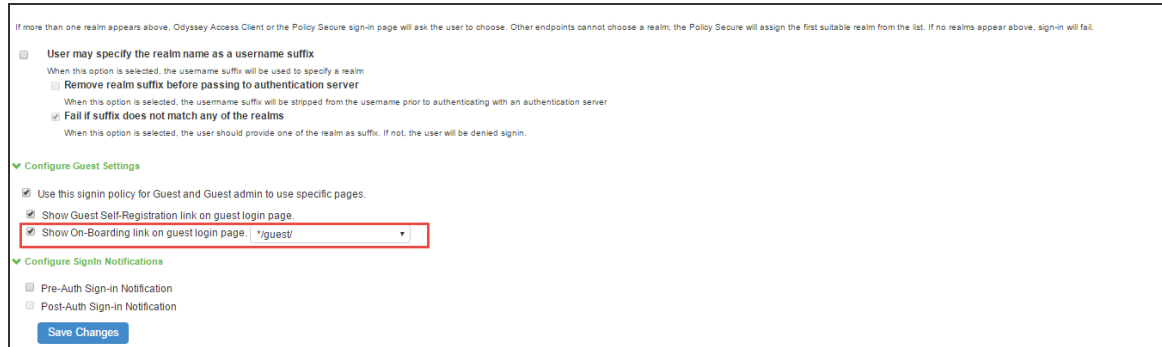
9. Select **User Realms > Guest Sponsor > Role Mapping** and make necessary changes and click **Save Changes** to save the settings.

Enabling Onboarding Feature

Enterprise onboarding feature provides automated onboarding of BYOD clients on premises (WLAN & LAN). IPS enables personal devices to be automatically configured for corporate access.

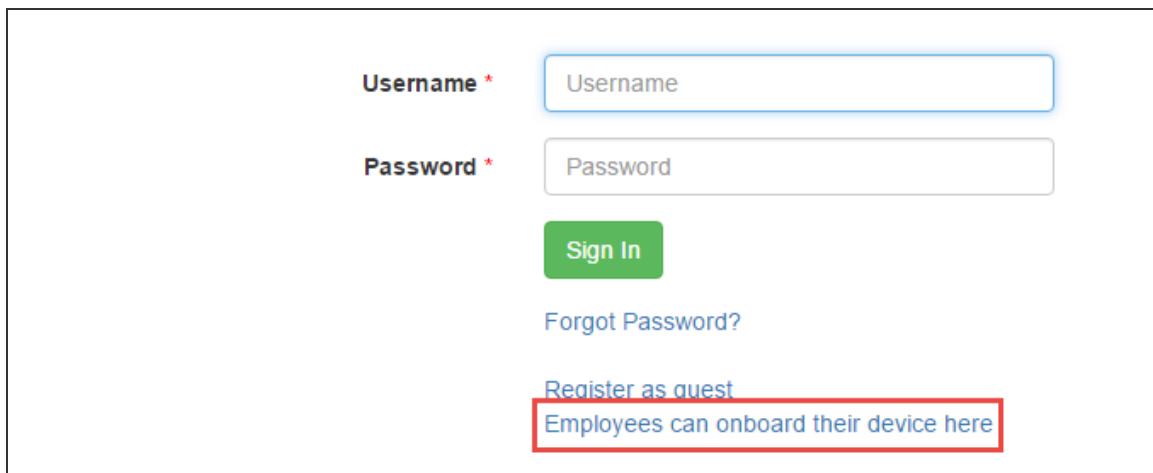
To enable this feature:

1. Select **Authentication > Signing In > Sign-in Policies**.
The Sign-in Polices tab displays the available sign-in policies.
2. Under the User URLs section select the default sign-in policy.



3. Select the Show On-Boarding link on guest log in page check box. A drop-down list appears next to it.
4. Select a required URL.
5. Click **Save Changes** to save the settings.

The Employees can onboard their device here link appears in an enterprise guest environment as shown in the following figure.



Localization

In a localized guest user environment when a user tries to register as a guest all the fields are displayed in that localized language, except the Company Name and Host or Sponsor fields which are displayed in English language.



French Language is used as an example.

To localize these two fields, an Admin user must enter the translated field names of Company Name and Host or Sponsor fields in the Guest Access Configurations section in IPS.

To make these changes:

Select **Authentication > Auth.Servers**. The Authentication Servers screen appears.

- Select a default Authentication Server to make the changes.
- The Settings tab of the Auth Server displays the settings.

Note: Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities

Guest Access

Guest User Account Managers

Enable Guest User Account Managers to administer Guest Accounts [Configure system GUAM settings](#)

Instructions for Guest User Account Manager: Instructions displayed for guest users creation and updation. You can use ,
, , <noscript>, and <a href= tags to format the text.

Maximum Account Validity Period: Set the Guest Account length limit (end time minus start time) in hours. This is valid for guests created by Guest Admin. Does not impact existing user expirations.

Guest Self-Registration

Send guest user credentials via: SMS Email [Configure SMS/Email settings](#)

Show credentials on screen after guest completes registration

Enable Sponsored Guest Access

Maximum Account Validity Period for Self Registered Guests: Set the Guest Account length limit in hours. This is valid for self registered guests. Does not impact existing user expirations.

Note: To enable Guest Self-Registration navigate to Signing In > Sign-in Policies > User URLs > [url] > [Configure Guest Settings](#)

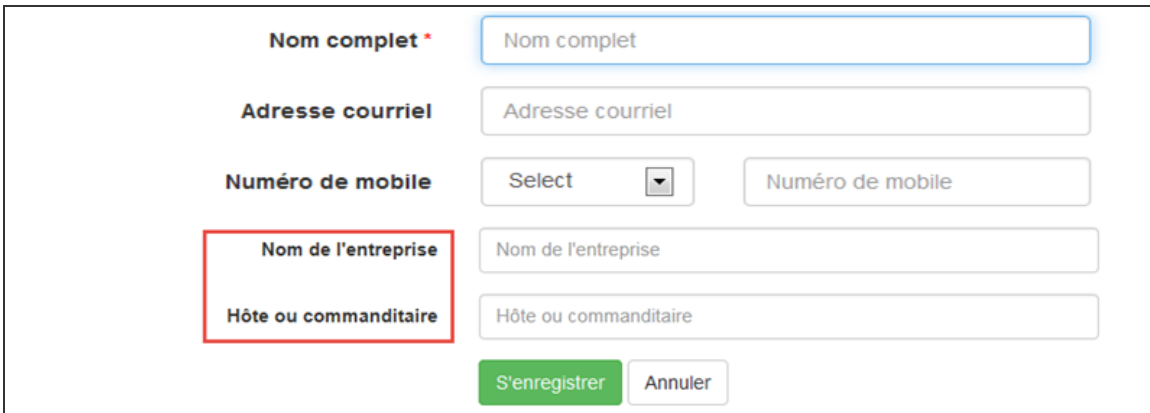
Common configuration for Guest User Account Managers and Guest Self-Registration

Guest User Name Prefix: Prefix applied to auto-generated user names.

Guest User Info Fields: Enter additional fields for guest user information, one field per line. For example:
Title
Company name
Sponsor

- In the Guest Access Configurations section, enter the translated field names of Company Name and Host or Sponsor fields in the Guest User Info Fields box.
- Click **Save Changes** to save the settings.

- In the enterprise guest environment when a guest tries to register, the Company Name and Host or Sponsor fields are displayed in the respective language.



The image shows a registration form with the following fields and labels:

- Nom complet ***: Input field with placeholder text "Nom complet".
- Adresse courriel**: Input field with placeholder text "Adresse courriel".
- Numéro de mobile**: A dropdown menu labeled "Select" and an input field with placeholder text "Numéro de mobile".
- Nom de l'entreprise**: Input field with placeholder text "Nom de l'entreprise".
- Hôte ou commanditaire**: Input field with placeholder text "Hôte ou commanditaire".

At the bottom of the form are two buttons: "S'enregistrer" (green) and "Annuler" (white).

Guest Self Registration

To enable Guest Self-Registration:

1. Select **Authentication > Signing In > Sign-in Policies > User URLs.**
2. Configure guest settings.

***/guest/**

User type: Users Administrators

Sign-in URL: Format: <host>-<path>/. Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: To create or manage pages, see [Sign-In pages](#).

Authentication realm

Specify what realms will be available when signing in.

	Available realms	Authentication protocol set	
<input type="checkbox"/>	Cert Auth	- Not applicable -	<input type="button" value="Add"/>
<input type="checkbox"/>	Guest	Guest	

If more than one realm appears above, Odyssey Access Client or the Policy Secure sign-in page will ask the user to choose. Other endpoints cannot choose a realm; the Policy Secure will assign the first suitable realm from the list. If no realms appear above, sign-in will fail.

User may specify the realm name as a Username suffix
When this option is selected, the Username suffix will be used to specify a realm

Remove realm suffix before passing to authentication server
When this option is selected, the username suffix will be stripped from the Username prior to authenticating with an authentication server

Fail if suffix does not match any of the realms
When this option is selected, the user should provide one of the realm as suffix. If not, the user will be denied sign-in.

Configure Guest Settings

Use this sign-in policy for Guest and Guest admin to use specific pages.

Show Guest Self-Registration link on guest login page.

Show On-Boarding link on guest login page.

3. Login as guest user and click **Register as Guest.**

Username *

Password *

[Forgot Password?](#)

4. Enter the name, email, contact number, company name, host or sponsor name.

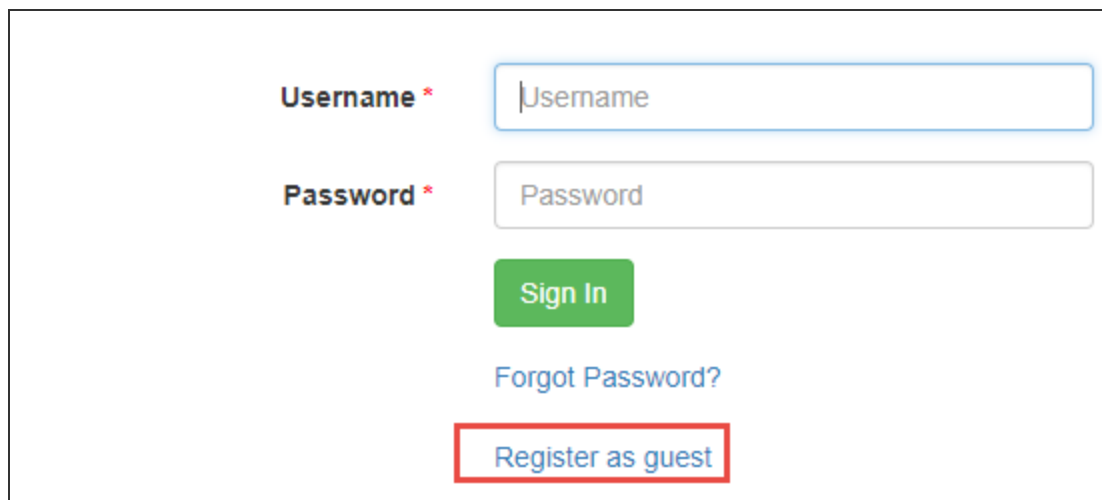
5. Click **Register**.

Guest Self Registration for Sponsor Approved Guest Access

The guest user logs in and registers as guest by entering the contact information such as name, email, phone, company name, sponsor name and the sponsor email who approves/denies the guest access. Once the sponsorer approves the access request. The Guest user can access the internet resources.

The user flow for sponsor approved guest access is described below:

1. Open the guest URL and click **Register as Guest**.



The screenshot displays a registration form with the following elements:

- Username ***: A text input field containing the placeholder text "Username".
- Password ***: A text input field containing the placeholder text "Password".
- Sign In**: A green button.
- Forgot Password?**: A blue text link.
- Register as guest**: A blue text link, which is highlighted with a red rectangular border.

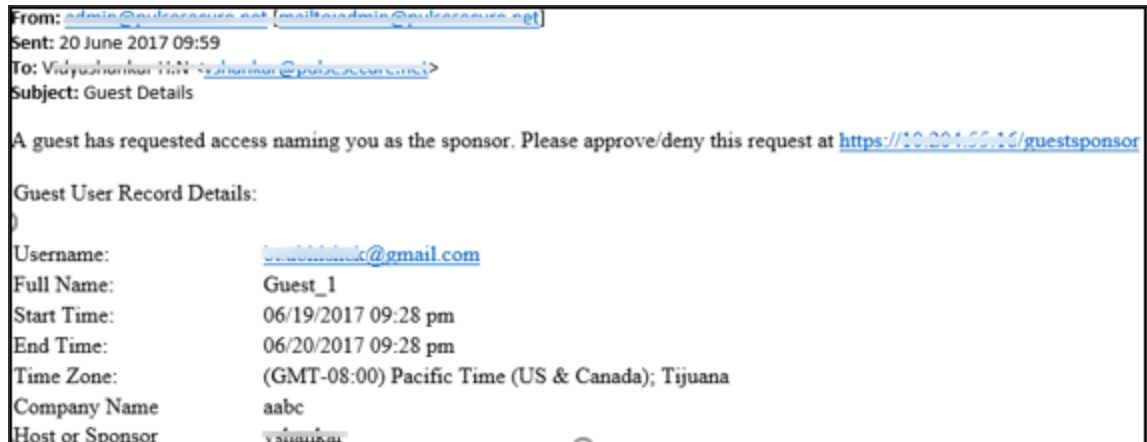
2. Enter the name, email, contact number, company name, host or sponsor name, and the sponsor email ID (Sponsored Guest Access) The sponsor email ID appears in the self-registration page only when the user enables Sponsored Guest Access option. See [Configuring IPS for Sponsored Guest Access](#).

The screenshot shows a registration form with the following fields: Full Name (*), Email, Mobile Number (with a dropdown for 'India' and a partial number '93'), Company Name, Host or Sponsor, and Sponsor Email (with a checkmark). A modal window is overlaid on the right, displaying the message: 'An account has been created for you.' Below this, it lists the 'Username: xyz@abc.com' and 'Password: Q3WMCAX5'. There is an 'OK' button in the bottom right of the modal. At the bottom of the form, there are 'Register' and 'Cancel' buttons.

3. The Guest user tries to open the Guest Account using the credentials. The user fails to login as the account should be approved by the Sponsorer.

The screenshot shows a login page. At the top, there is a red banner with the text 'Waiting for Approval'. Below this, there are two input fields: 'Username *' and 'Password *'. A green 'Sign In' button is positioned below the password field. Below the button, there are two links: 'Forgot Password?' and 'Register as guest'.

- The Sponsor user receives an email notification to validate the Guest user.



- The Sponsorer logs in with the user credentials and opens the Sponsor Portal to view the list of Guest users.



The Sponsorer login name must match with the sponsor email ID or AD username as entered by the guest while self registering.

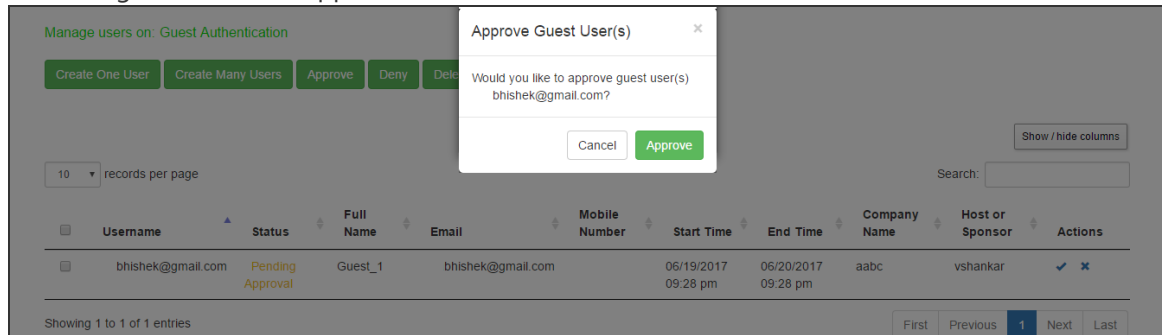
Manage users on: Guest Authentication

100 records per page Show / hide columns

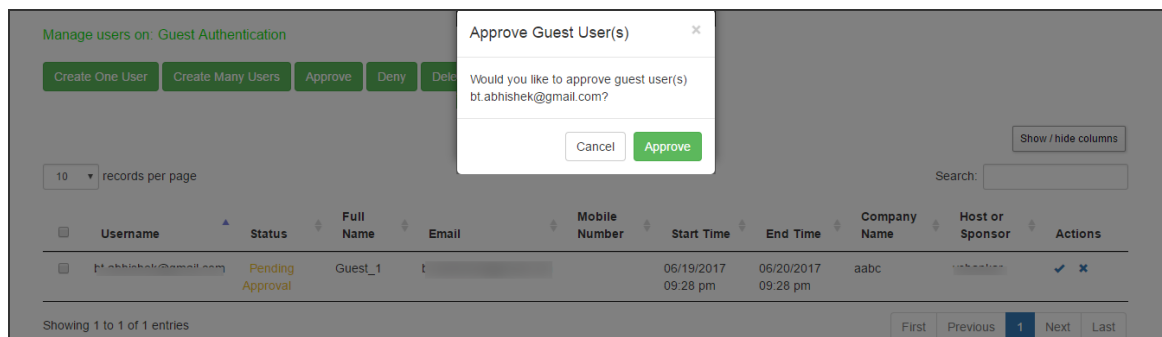
Search:

Username	Status	Full Name	Email	Mobile Number	Start Time	End Time	Company Name	Sponsor Name	Actions
guest_3200	Pending Approval		xyz@xyz.com		05/25/2017 01:58 pm	05/26/2017 01:58 pm			
guest_3202	Pending Approval		abc@abc.com		05/25/2017 01:59 pm	05/26/2017 01:59 pm			
guest_3204	Pending Approval	Prakesh	prakesh@pulsoaccess.net		05/25/2017 02:03 pm	05/26/2017 02:03 pm	abc	xyz	
guest_3199	Pending Approval		pqr@pqr.com		05/25/2017 01:58 pm	05/26/2017 01:58 pm			
vidyaashankar@gmail.com	Pending Approval	vidyaashankar	vidyaashankar@gmail.com		05/25/2017 03:02	05/26/2017 03:02	Juniper	vidyaashankar	

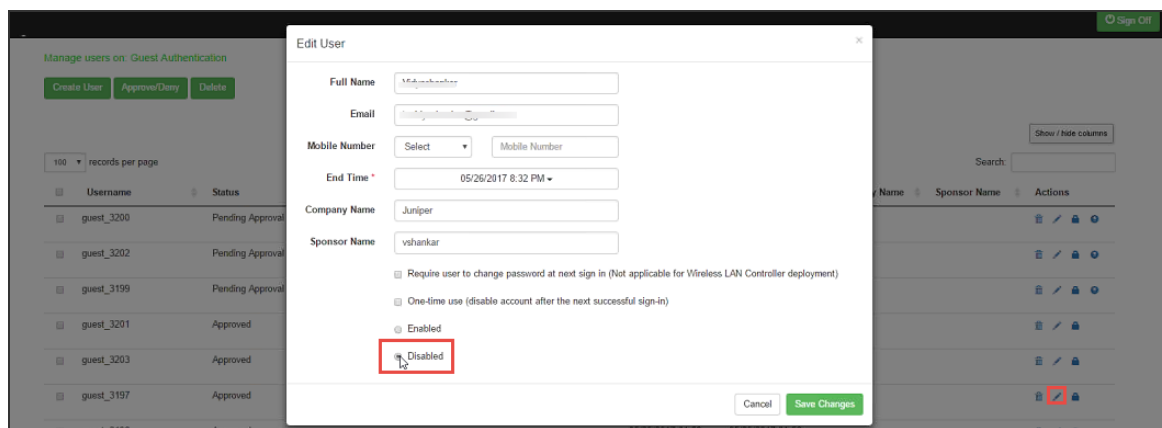
- From the Sponsor page, the Sponsor user can click **Approve** to approve the guest user account details. Figure shows the Approve window.



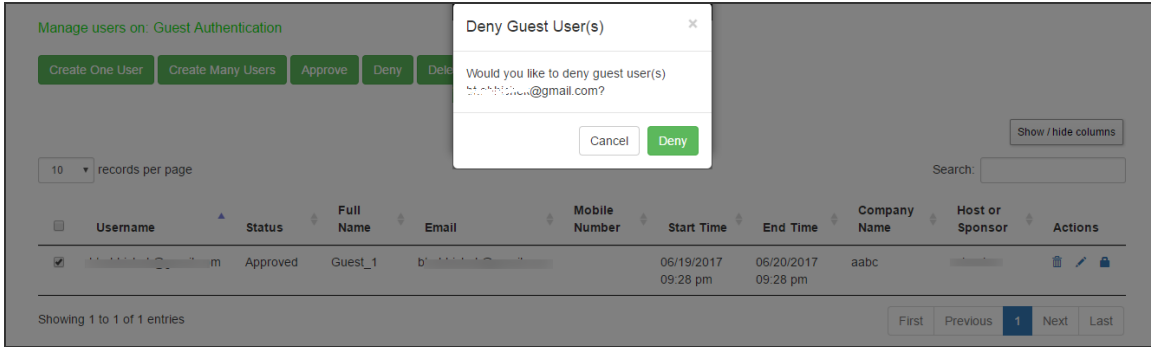
- Click **Approve**. The Guest User receives a notification email describing that the access is approved.



- The Sponsor has the flexibility to edit the user details as shown in figure. For example, the Sponsorer can revoke the access by changing the setting to disabled.



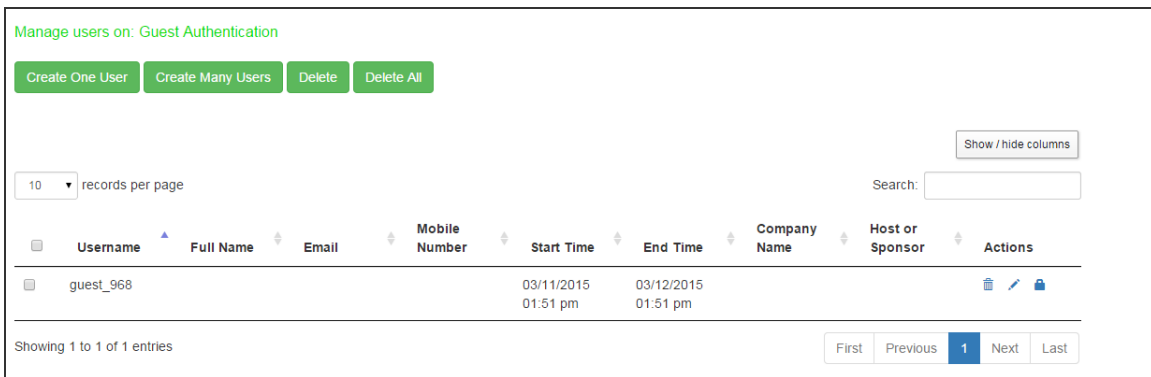
The following page is displayed if the Sponsor chooses to deny access to the Guest User. A notification email is sent to the Guest User describing that the access is denied.



Guest User Administration

Creating Guest User Accounts

When the guest user account manager (GUAM) logs in through the sign-in page for the guest realm, an interface is presented for creating accounts as shown in the following figure. The GUAM can view all the guest users created by the GUAM, self registered, and sponsor created users.





Settings	Guidelines
Create One User	Creates one user
Create Many Users	Creates multiple users
Delete	Deletes the selected users
Delete All	Deletes all the users on the page.
Show / hide columns	Select the option to hide or show specific columns.
Delete	Deletes the record of the guest user.

Settings	Guidelines
Reset	Resets the password of the guest user.
Edit	Edits the details of the guest user.
Search	Searches for guest/s with specific names.

The following figure shows the page for adding a single guest user.


Settings	Guidelines
Username	Specify an account username. If the local authentication server has been configured with a prefix for guest accounts, the username box is populated with the next username in the prefix-based sequence. We recommend you retain the guest_ prefix so that you can rely on the naming convention in your role mapping rules.
Full Name	Specify the name of the guest.
Password	A strong password is generated automatically, or you can specify a different password. After you have saved the configuration, the system displays the password characters as asterisks (*) instead of blanks or cleartext.

Settings	Guidelines
	<p> The password cannot be decrypted later unless the appropriate option is set when you create a local authentication server.</p>
Mobile Number	Select the country name and then specify a valid phone number of the guest user. The IPS sends the login credentials to this mobile number through SMS.
Email	Specify an email address you can use to contact the guest if necessary.
Start Time	By default, the 'Now' option is displayed. You can specify a start time for the account activity period by clicking on the drop-down and selecting from the calendar menu.
End Time	<p>By default, 'After 24 hours is displayed. You can specify an end of the account activity period. Click on the drop-down menu and select from the calendar menu. Once a user account has expired, it is deleted from the system.</p> <p>The process that deletes the guest user account runs every ten minutes. There may be a delay of some minutes before the account is purged. Even if the time or date on the system is moved ahead past the expiration time, the account could still be valid until the purge process runs. One-time user accounts are not affected by the ten-minute delay: one-time accounts are deleted immediately after the user exits.</p>
Company Name	Enter the name of the company of the guest.
Host or Sponsor	Enter whether the guest is a Host or Sponsor.
One-time use	Select this option if you want the account deleted immediately after the guest user exits the browser or signs out.
Enabled	Select this option to enable the account
Require user to change password at next sign in	<p><u>Select this option to prompt the user to change the configured password.</u></p> <p> This option will not be supported in GUAM for WLC case. This option should not be enabled. Even if enabled, it will not have any effect.</p>

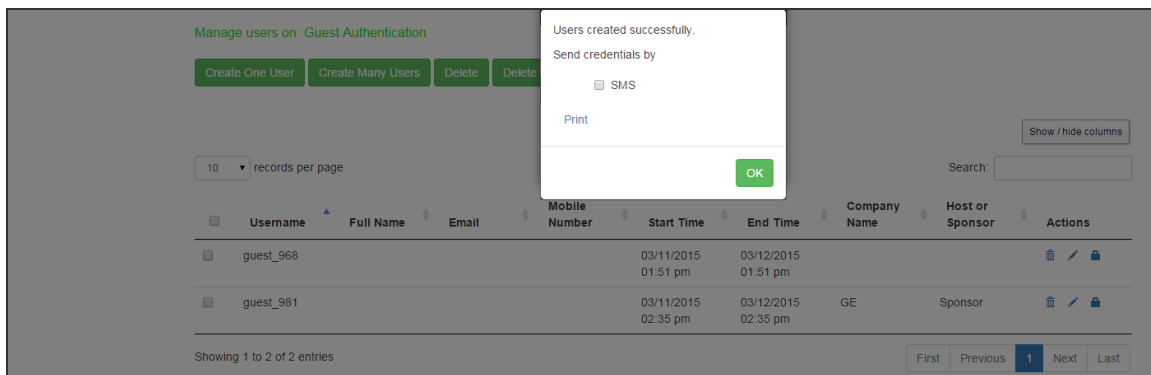
The following figure shows the page for adding many users and table describes the user configuration.

The guest usernames and passwords are created by the system as you click in the Username text box.

Settings	Guidelines
Username	Specify the prefix to be used for the multiple accounts you are creating.
Full Name	Enter the full name of the guest.
Password	A strong password is generated automatically, or you can specify a different password. After you have saved the configuration, the system displays the password characters as asterisks (*) instead of blanks or cleartext.
Start Time	You can specify a start time for the account activity period by clicking on the drop-down and selecting from the calendar menu
End Time	You can specify an end of the account activity period. Click on the drop-down menu and select from the calendar menu. Once a user account has expired, it is deleted from the system.

Settings	Guidelines
	The process that deletes the guest user account runs every ten minutes. There may be a delay of some minutes before the account is purged. Even if the time or date on the system is moved ahead past the expiration time, the account could still be valid until the purge process runs. One-time user accounts are not affected by the ten-minute delay: one-time accounts are deleted immediately after the user exits.
Company Name	Enter the name of the company of the guest. (Optional)
Host or Sponsor	Enter whether the guest is a Host or Sponsor. (Optional)
One-time use	Select this option if you want the account deleted immediately after the guest user exits the browser or signs out
Enabled	Select this option to enable the account.
Require user to change password at next sign in	<p><u>Select this option to prompt the user to change the configured password</u></p> <p> This option will not be supported in GUAM for WLC case. This option should not be enabled. Even if enabled, it will not have any effect.</p>

After the GUAM user clicks the Create button the following popup is displayed.



1. Select **SMS** and click **OK** to send the credentials to the guests' mobiles.
2. Click **Print** to generate a printout of the credentials.

Manage users on: Guest Authentication

10 records per page Show / hide columns

Search:

<input type="checkbox"/>	Username	Full Name	Email	Mobile Number	Start Time	End Time	Company Name	Host or Sponsor	Actions
<input type="checkbox"/>	guest_968				03/11/2015 01:51 pm	03/12/2015 01:51 pm			<input type="button" value="Print"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	guest_981				03/11/2015 02:35 pm	03/12/2015 02:35 pm	GE	Sponsor	<input type="button" value="Print"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	guest_992			+ (1) 18883145822	03/11/2015 03:16 pm	03/12/2015 03:16 pm			<input type="button" value="Print"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	guest_993				03/11/2015 03:16 pm	03/12/2015 03:16 pm			<input type="button" value="Print"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	guest_994				03/11/2015 03:16 pm	03/12/2015 03:16 pm			<input type="button" value="Print"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	guest_995				03/11/2015 03:16 pm	03/12/2015 03:16 pm			<input type="button" value="Print"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Showing 1 to 6 of 6 entries First Previous **1** Next Last

From the GUAM page, the GUAM user can click Edit icon of a guest user account to modify the guest user account details. Table shows the Edit User window.

Manage users on: Guest Authentication

10 records per page

Edit User x

Full Name
Email
Mobile Number
End Time *
Company Name
Host or Sponsor

Require user to change password at next sign in
 One-time use (disable account after the next successful sign-in)
 Enabled
 Disabled

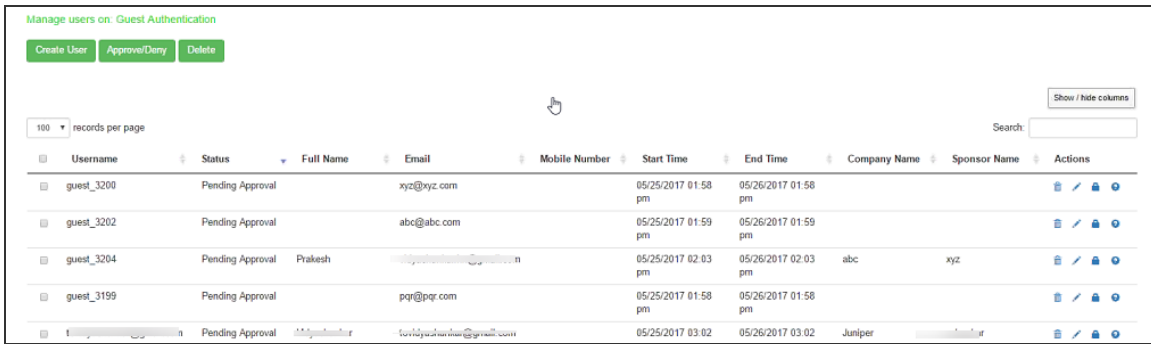
After clicking **Save Changes** the following popup appears.

From the GUAM page, the GUAM user can click Print to generate a printable record of the guest user account. Figure shows the print details page.

Guest User Record Details:	
Username:	guest_981
Full Name:	John
Password:	*****
Start Time:	03/11/2015 02:35 pm
End Time:	03/12/2015 02:35 pm
Company Name	GE
Host or Sponsor	Sponsor

Creating Guest Sponsor Portal


The Sponsor page is similar to GUAM page, where the Sponsor can see the list of guest users who marked the Sponsor while creating the guest user account. When the guest sponsor logs in through the sign-in page for the guest sponsor realm the following page is displayed for creating accounts. The Sponsor can see only the guest users created by the Sponsor and the Guest users who have marked someone as a Sponsor while creating guest user account.




The following table describes the various fields on the Sponsor user page.

Settings	Guidelines
Create One User	Creates one user
Create Many Users	Creates multiple users
Approve	Approves the guest user access.
Deny	Denies the guest user access.
Delete	Deletes the selected users
Delete All	Deletes all the users on the page.
Show / hide columns	Select the option to hide or show specific columns.
Delete	Deletes the record of the guest user.
Reset	Resets the password of the guest user.
Edit	Edits the details of the guest user.
Search	Searches for guest/s with specific names.

The following figure shows the page for adding a single guest user.


Settings	Guidelines
Username	Specify an account username. If the local authentication server has been configured with a prefix for guest accounts, the username box is populated with the next username in the prefix-based sequence. We recommend you retain the guest_ prefix so that you can rely on the naming convention in your role mapping rules.
Full Name	Specify the name of the guest.
Password	<p>A strong password is generated automatically, or you can specify a different password. After you have saved the configuration, the system displays the <u>password characters as asterisks (*) instead of blanks or cleartext.</u></p> <p> The password cannot be decrypted later unless the appropriate option is set when you create a local authentication server.</p>
Mobile Number	Select the country name and then specify a valid phone number of the guest user. The IPS sends the login credentials to this mobile number through SMS.
Email	Specify an email address you can use to contact the guest if necessary.
Start Time	By default, the 'Now' option is displayed. You can specify a start time for the account activity period by clicking on the drop-down and selecting from the calendar menu.

Settings	Guidelines
End Time	<p>By default, 'After 24 hours is displayed. You can specify an end of the account activity period. Click on the drop-down menu and select from the calendar menu. Once a user account has expired, it is deleted from the system.</p> <p>The process that deletes the guest user account runs every ten minutes. There may be a delay of some minutes before the account is purged. Even if the time or date on the system is moved ahead past the expiration time, the account could still be valid until the purge process runs. One-time user accounts are not affected by the ten-minute delay: one-time accounts are deleted immediately after the user exits.</p>
Company Name	Enter the name of the company of the guest.
Host or Sponsor	Enter whether the guest is a Host or Sponsor.
One-time use	Select this option if you want the account deleted immediately after the guest user exits the browser or signs out.
Enabled	Select this option to enable the account
Require user to change password at next sign in	<p>Select this option to prompt the user to change the configured password.</p> <hr/> <p> This option will not be supported in GUAM for WLC case. This option should not be enabled. Even if enabled, it will not have any effect.</p> <hr/>

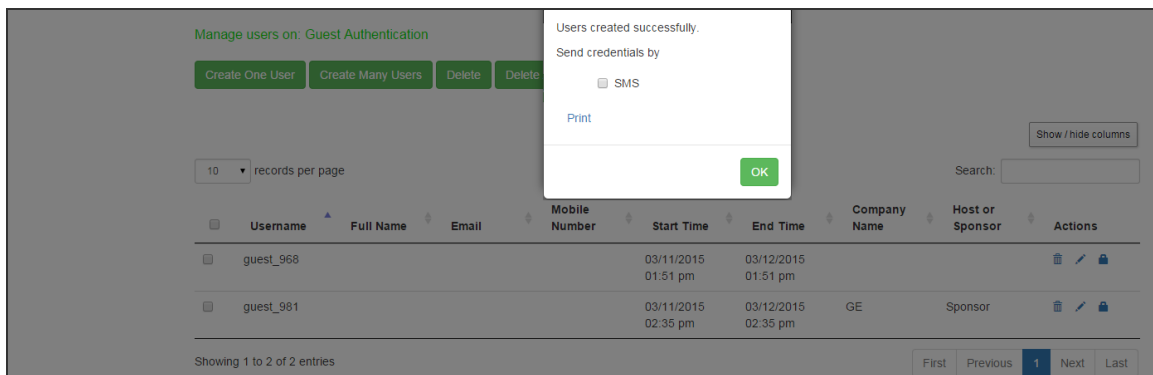
The following figure shows the page for adding many users and table describes the user configuration.

The guest usernames and passwords are created by the system as you click in the Username text box.

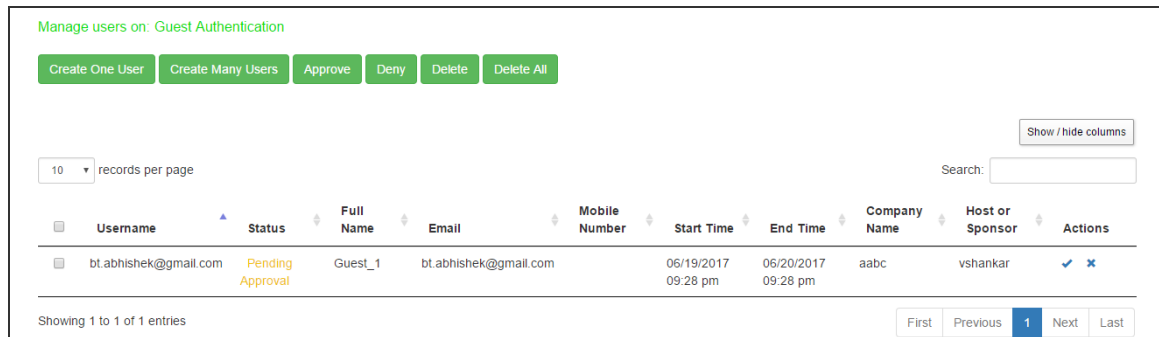
Settings	Guidelines
Username	Specify the prefix to be used for the multiple accounts you are creating.
Full Name	Enter the full name of the guest.
Password	A strong password is generated automatically, or you can specify a different password. After you have saved the configuration, the system displays the password characters as asterisks (*) instead of blanks or cleartext.
Start Time	You can specify a start time for the account activity period by clicking on the drop-down and selecting from the calendar menu
End Time	You can specify an end of the account activity period. Click on the drop-down menu and select from the calendar menu. Once a user account has expired, it is deleted from the system.

Settings	Guidelines
	The process that deletes the guest user account runs every ten minutes. There may be a delay of some minutes before the account is purged. Even if the time or date on the system is moved ahead past the expiration time, the account could still be valid until the purge process runs. One-time user accounts are not affected by the ten-minute delay: one-time accounts are deleted immediately after the user exits.
Company Name	Enter the name of the company of the guest. (Optional)
Host or Sponsor	Enter whether the guest is a Host or Sponsor. (Optional)
One-time use	Select this option if you want the account deleted immediately after the guest user exits the browser or signs out
Enabled	Select this option to enable the account.
Require user to change password at next sign in	<p><u>Select this option to prompt the user to change the configured password</u></p> <p> This option will not be supported in GUAM for WLC case. This option should not be enabled. Even if enabled, it will not have any effect.</p>

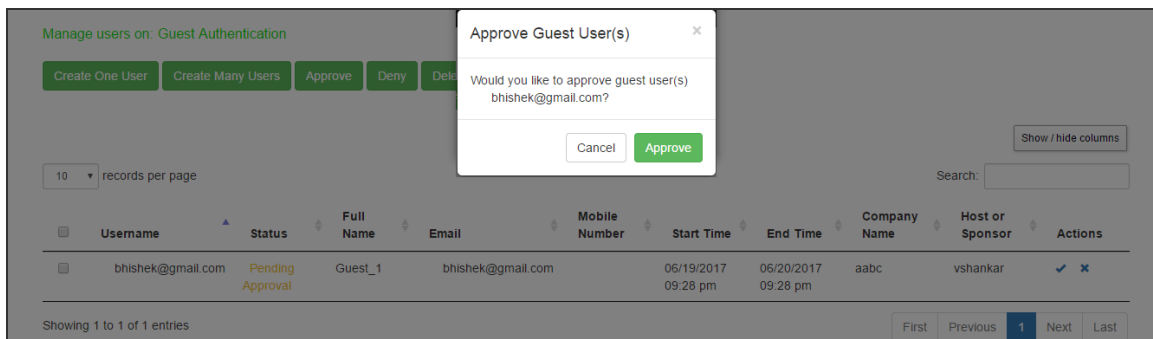
After the GUAM user clicks the Create button the following popup is displayed.



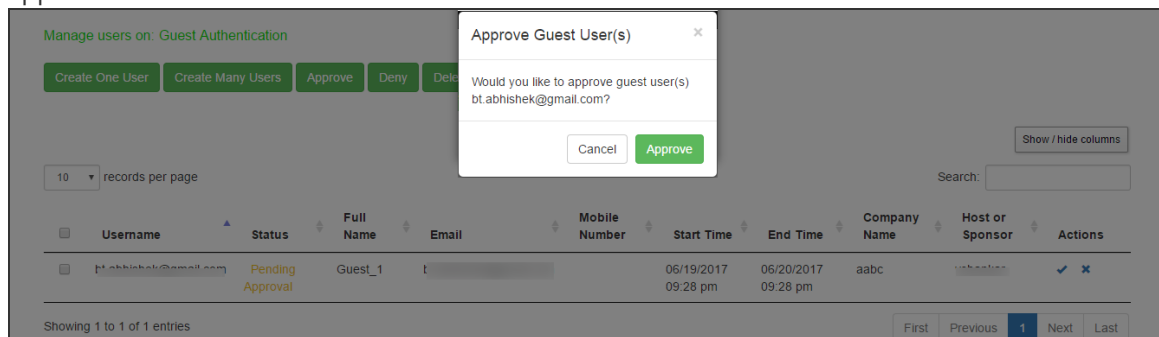
1. Select SMS and click OK to send the credentials to the guests' mobiles.
2. Click Print to generate a printout of the credentials.



From the Sponsor page, the Sponsor user can click Approve icon of a guest user account to approve the guest user account details. The following figure shows the Approve window.

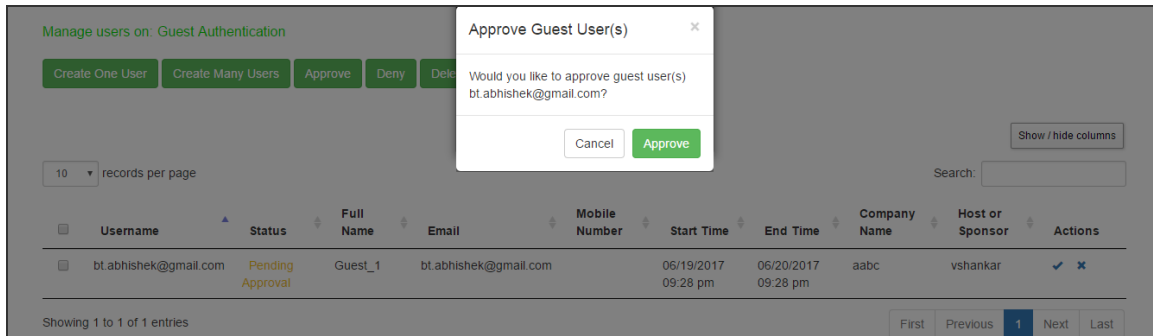


1. Click Approve. The Guest User receives a notification email describing that the access is approved.



The Sponsor has the flexibility to edit the user details as shown below.

The following page is displayed if the Sponsor chooses to deny access to the Guest User. A notification email is sent to the Guest User describing that the access is denied.



Customizing Guest Self Registration User Pages

The customization for GUAM is no more supported from the IPS 5.2 release.

This topic describes how to customize the Guest Self Register page. It includes the following information:

- Downloading the Sample Template Files
- Modifying the Sample Template Files
- Uploading Your Customized Files
- Using the Customized Pages
- Verifying the Customization

Downloading the Sample Template Files

The sample template zip file includes the following files which are added for the IPS 5.2 release:

- GuestLoginPage.thtml
- GuestLogout.thtml
- GuestSelfRegistration.thtml
- GuestForgotPassword.thtml
- GuestSigninNotifPreAuth.thtml

To download the sample template files:

1. Select **Authentication > Signing In > Sign in** pages. The Signing In screen appears.
2. Click **Upload Custom Pages**.
3. The **Upload Custom Sign-In Pages** screen appears. This page hosts the sample.zip files which can be used to customize the guest sign in pages.
4. Click the Sample link in the Sample Template Files pane.
5. Download the latest sample.zip file.

Modifying the Sample Template Files

You can edit the HTML to modify the look and feel of your page. You can add, modify, or delete JavaScript functions and variables to customize the functionality presented on your page. This section provides examples of common customizations for Guest Self Registration pages. For a reference on the files, functions, and variables found in the templates included in the sample.zip file, see the Custom Sign-In Pages Developer Reference.

Figure shows the contents of the GuestSelfRegistration.html file. The JavaScript functions and variables used for the standard user interface controls that appear in the predefined pages are highlighted in bold.

Table describes some of the common variables used in the templates and their meaning.

Variable	Definition
I18N_FULL_NAME	Field for entering the full name of guest user.
I18N_USERNAME_ADMIN_EMAIL	Field for entering the email id of guest user.
I18N_USER_ADMIN_MOBILE_NUMBER	Field for entering mobile number of guest user.
I18N_USER_ADMIN_REGISTER	Register option in the Guest Self Registration page. Click the button after entering the user details.
I18N_CANCEL	Cancel option. Cancels the registration process and takes the user back to the Sign In page of Guest User
I18N_USERNAME_COLON	Username: field. It displays the username in the confirmation box.

Variable	Definition
I18N_PASSWORD_COLON	Password: field. It displays the password in the confirmation box.
I18N_USER_ADMIN_CREATING_ACCOUNT	Displays the message "An account has been created for you" in the confirmation box.

```

<div id= "fnDiv" class="form-group required">
  <label for="fullname" class="col-sm-2 control-label"><% I18N_FULL_NAME %></label>
  <div id="fnDiv2" class="col-sm-5">
    <input type="text" class="form-control" id="fullname" name="fullname"
placeholder="<% I18N_FULL_NAME %>" autofocus validate>
  </div>
</div>
<div id= "emailDiv" class="form-group <%IF emailRequired == 1%> required <%END%>">
  <label for="email" class="col-sm-2 control-label"><% I18N_USER_ADMIN_EMAIL
%></label>
  <div id="emailDiv2" class="col-sm-5">
    <input type="email" class="form-control" id="email" name="email" placeholder="<%
I18N_USER_ADMIN_EMAIL %>" validate>
  </div>
</div>
<div id= "mnDiv" class="form-group <%IF smsRequired == 1%> required <%END%>">
  <label for="mobilenumber" class="col-sm-2 control-label"><% I18N_USER_ADMIN_
MOBILE_NUMBER %></label>
  <div id="mnDiv1" class="col-sm-2">
    <select id="cmbCountryCode" class="form-control" name="cmbCountryCode"
<%disabled%>>
      <% FOREACH country = countryCode %>
        <option id="<% country.id %>" value="<% country.id %>" <%IF
countrySelected == country.id%> selected <%END%>> <% country.name %> </option>
      <%END%>
    </select>
  </div>
  <div id="mnDiv2" class="col-sm-3">
    <input type="tel" class="form-control" id="mobilenumber" name="mobilenumber"
placeholder="<% I18N_USER_ADMIN_MOBILE_NUMBER %>" validate>
  </div>
</div>

```

Removing Fields

You can remove fields from the user interface form by deleting the HTML and JavaScript that define them from the sample file. For example, to delete the "Email" option box, delete the following HTML and variables:

Example

```
<div id= "emailDiv" class="form-group <%IF emailRequired == 1%> required <%END%>">
  <label for="email" class="col-sm-2 control-label"><% I18N_USER_ADMIN_EMAIL
%></label>
  <div id="emailDiv2" class="col-sm-5">
    <input type="email" class="form-control" id="email" name="email" placeholder="<%
I18N_USER_ADMIN_EMAIL %>" validate>
  </div>
</div>
```



Never delete or modify the following required variables:

```
Guest_Includes-
signinAgainUrl-
LoginPageErrorMessage-Specifies the error message. The device generates the error
message in case of an error otherwise it will be empty
preAuthSNTText
```

The screenshot shows a registration form with the following fields and controls:

- Full Name ***: A text input field.
- Email**: A text input field.
- Mobile Number**: A dropdown menu with "Select" and a downward arrow, followed by a text input field labeled "Mobile Number".
- Company Name**: A text input field.
- Host or Sponsor**: A text input field.
- Buttons**: A green "Register" button and a white "Cancel" button.



You can add a field in the html to display messages

Figure shows the result of the customization

The screenshot shows a registration form with the following elements:

- Full Name ***: A text input field.
- Mobile Number**: A dropdown menu with 'Select' and a downward arrow, followed by a text input field containing 'Mobile Number'.
- Company Name**: A text input field containing 'Company Name'.
- Host or Sponsor**: A text input field containing 'Host or Sponsor'.
- Buttons**: A green 'Register' button and a white 'Cancel' button.

Editing Fields

You can edit fields in the user interface form by editing the HTML and JavaScript that define them from the sample file. For example, to edit the “Mobile Number” option box as ‘Contact Number”, edit the following HTML and variables:

Script Before Editing

```
<div id= "mnDiv" class="form-group <%IF smsRequired == 1%> required <%END%>">
  <label for="mobilenumber" class="col-sm-2 control-label"> <% I18N_USER_ADMIN_
MOBILE_NUMBER %>Contact Number</label>
  <div id="mnDiv1" class="col-sm-2">
    <select id="cmbCountryCode" class="form-control" name="cmbCountryCode"
<%disabled%>>
      <% FOREACH country = countryCode %>
        <option id="<% country.id %%" value="<% country.id %%" <%IF
countrySelected == country.id%> selected <%END%>> <% country.name %> </option>
      <%END%>
    </select>
  </div>
  <div id="mnDiv2" class="col-sm-3">
    <input type="tel" class="form-control" id="mobilenumber" name="mobilenumber"
placeholder="<% I18N_USER_ADMIN_MOBILE_NUMBER %%" validate>
  </div>
</div>
```

Script After Editing

```
<div id= "mnDiv" class="form-group <%IF smsRequired == 1%> required <%END%>">
  <label for="mobilenumber" class="col-sm-2 control-label"> Contact Number</label>
  <div id="mnDiv1" class="col-sm-2">
```

```

    <select id="cmbCountryCode" class="form-control" name="cmbCountryCode"
    <%disabled%>>
      <% FOREACH country = countryCode %>
        <option id="<% country.id %>" value="<% country.id %>" <%IF
countrySelected == country.id%> selected <%END%>> <% country.name %> </option>
      <%END%>
    </select>
  </div>
  <div id="mnDiv2" class="col-sm-3">
    <input type="tel" class="form-control" id="mobilenumber" name="mobilenumber"
placeholder="Contact Number" validate>
  </div>
</div>

```

Figure shows the result of the customization

The screenshot shows a registration form with the following fields and controls:

- Full Name ***: A text input field with a vertical cursor.
- Email**: A text input field with the placeholder text "Email".
- Contact Number**: A dropdown menu with "Select" and a downward arrow, followed by a text input field with the placeholder text "Contact Number".
- Company Name**: A text input field with the placeholder text "Company Name".
- Host or Sponsor**: A text input field with the placeholder text "Host or Sponsor".
- Buttons**: A green "Register" button and a white "Cancel" button.

Uploading Your Customized Files

After you have edited the sample template files, save the files with the same name and add them to the sample.zip file (replacing the previous files).

To upload the files to the system:

1. Select **Signing In > Sign-in pages**.
2. Click **Browse** to select the sample.zip file containing the custom templates and assets.
3. Click **Upload Custom Pages**.
4. The Upload Custom Sign-In Pages screen appears.

Setting	Guidelines
Sign-In Pages	
Name	Specify the name for the sign-in page.
Page Type	Specify the page type. Access is selected by default.
Template File	Select the template file in zipped format that contains the custom templates and assets.
Upload	
Skip validation checks during upload	Select this option to skip the validation checks for the template file.
Upload Custom Pages	Select this option to upload the custom pages.

Using the Customized Pages

After you have uploaded the customized files, you can associate them with your Guest Self Registration sign-in page.

To use the customized pages:

1. Select **Authentication > Signing-In > Sign-In Policies** to display the sign-in policies configuration page.
2. Select the custom sign-in page from the drop-down list..
3. Click **Save Changes**.

Verifying the Customization

Sign in to the Guest Self Registration sign-in page as a guest user account manager and verify that the customizations you have made were applied.

Figure shows the customized Guest Self Registration page, without the Email ID field, and the Mobile Number field changed as Contact Number.

Full Name *

Contact Number

Company Name

Host or Sponsor

Configuring Cisco 2500 WLC

Configuring Cisco WLC for IPS GUAM and Guest Self-Registration

This section explains the steps to configure Cisco 2500 WLC for deploying IPS GUAM and Guest Self-Registration feature. This section provides examples of how to configure the Cisco WLC. For more information, see Cisco documentation.

Configuration Required on Cisco WLC for Local AP mode

Configuring RADIUS server

1. Login to Cisco WLC. Select **Security > AAA > RADIUS**. Configure IPS server as authentication and accounting servers.

2. Support for RFC 3576 - Enable this option to trigger RADIUS disconnect when required.

Auth Servers > Guest Authentication

Guest Authentication

Settings Users Admin Users

*Name: Label to reference this server.

▼ Password Options

Minimum length: characters

Maximum length: characters

Password must have at least digits

Password must have at least letters

Password must have mix of UPPERCASE and lowercase letters

Password must be different from username

New passwords must be different from previous password

Password stored as clear text This option can only be set during create

Note: If password stored as clear text, more authentication protocols, i.e. CHAP, EAP-MD5, are supported

▼ Password Management

Allow users to change their passwords

Force password change after days

Prompt users to change their password days before current password expires

Note: Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities

▼ Guest Access

Guest User Account Managers

Enable Guest User Account Managers to administer Guest Accounts Configure system GUAM settings

Instructions for Guest User Account Manager:

Instructions displayed for guest users creation and updation. You can use ,
, , <noscript>, and tags to format the text.

Maximum Account Validity Period: Set the Guest Account length limit (end time minus start time) in hours. This is valid for guests created by Guest Admin. Does not impact existing user expirations.

Guest Self-Registration

Send guest user credentials via: SMS

Email Configure SMS/Email settings

Show credentials on screen after guest completes registration

Enable Sponsored Guest Access

Response message for the Sponsor: This message will be sent as email to the sponsor.

Approve message for the Guest: This message will be sent as email/SMS to the guest user.

Deny message for the Guest: This message will be sent as email/SMS to the guest user.

Maximum Account Validity Period for Self Registered Guests: Set the Guest Account length limit in hours. This is valid for self registered guests. Does not impact existing user expirations.

Note: To enable Guest Self-Registration navigate to Signing In > Sign-in Policies > User URLs > [url] > Configure Guest Settings

Common configuration for Guest User Account Managers and Guest Self-Registration

Guest User Name Prefix: Prefix applied to auto-generated user names.

Guest User Info Fields: Enter additional fields for guest user information, one field per line. For example:
Title
Company name
Sponsor

* indicates required field

The screenshot shows the Cisco WLC configuration interface for a new RADIUS Authentication Server. The left sidebar shows the navigation menu with 'Security' selected. The main content area is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

- Server Index (Priority): 3
- Server IP Address: 3.3.3.2
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576: Enabled
- Server Timeout: 2 seconds
- Network User: Enable
- Management: Enable
- IPsec: Enable

Using CLI

Before creating the radius server, you need to allot an index number to it which is not currently in use. To find out the index numbers which are currently in use in WLC, use the following command:

```
show radius summary
```

Go through the authentication servers and accounting servers section in the displayed output. Use an unused index number for adding radius authentication or accounting server.

```
config radius auth add <RADIUS auth server ID> <RADIUS server IP> 1812 ascii
<password>
config radius auth disable < RADIUS auth server ID >
config radius auth rfc3576 enable < RADIUS auth server ID >
config radius auth enable < RADIUS auth server ID >
config radius acct add <RADIUS acct server ID > <RADIUS server IP> 1813 ascii
<password>
```

Configuring ACLs

1. On the CISCO WLC main screen go to **Security > Access Control Lists**. Create an IPv4 ACL list to allow DNS, DHCP and IPS (Traffic).

The screenshot shows the Cisco WLC configuration interface for 'Access Control Lists > Edit'. The 'General' tab is active, showing the 'Access List Name' as 'test' and 'Deny Counters' as 0. Below this is a table of rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DHCP Client	Any	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DHCP Server	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	Any	Any	Any	0
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
5	Permit	3.3.3.0 / 255.255.255.0	3.3.3.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

Using CLI

To see all the ACLs that are configured on the controller enter the following command:

```
show acl summary
```

To create an ACL with name test

```
config acl create test
```

To create a rule in the test ACL

```
config acl rule add test 1 # Creating Rule No 1
```

```
config acl rule protocol test 1 17 # 17 is UDP protocol
```

```
config acl rule source port range test 1 68 68 # 68 is DHCP client port number
```

```
config acl rule action test 1 permit # Allow access
```

```
config acl rule add test 2 # Creating Rule No 2
```

```
config acl rule protocol test 2 17
```

```
config acl rule source port range test 2 67 67 # 67 is DHCP server port number
```

```
config acl rule action test 2 permit
```

```
config acl rule add test 3 # Creating Rule No 3
```

```
config acl rule protocol test 3 17
```

```
config acl rule source port range test 3 53 53 # Port 53 for DNS
```

```
config acl rule action test 3 permit
```

```
config acl rule add test 4 # Creating Rule No 4
```

```
config acl rule protocol test 4 17
```

```
config acl rule destination port range test 4 53 53
```

```
config acl rule action test 4 permit
```

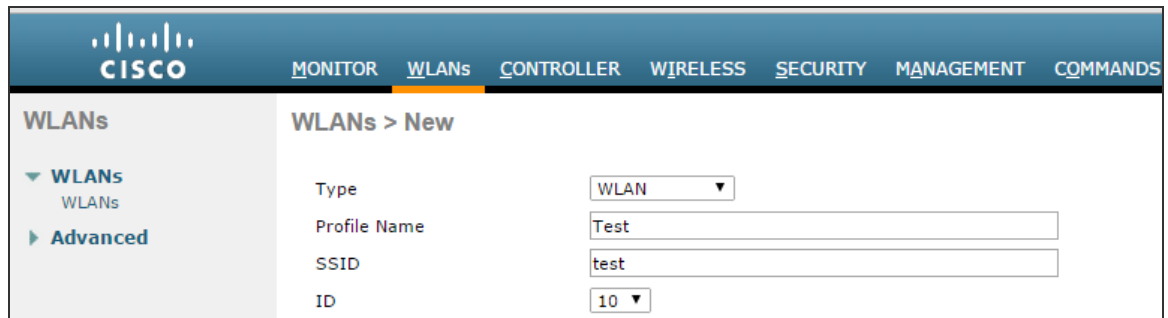
```
config acl rule add test 5 # Creating Rule No 5
config acl rule source address test 5 3.3.3.2 255.255.255.255
config acl rule action test 5 permit
```

```
config acl rule add test 6 # Creating Rule No 6
config acl rule destination address test 6 3.3.3.2 255.255.255.255
config acl rule action test 6 permit
```

Configuring WLAN

To configure Cisco WLAN:

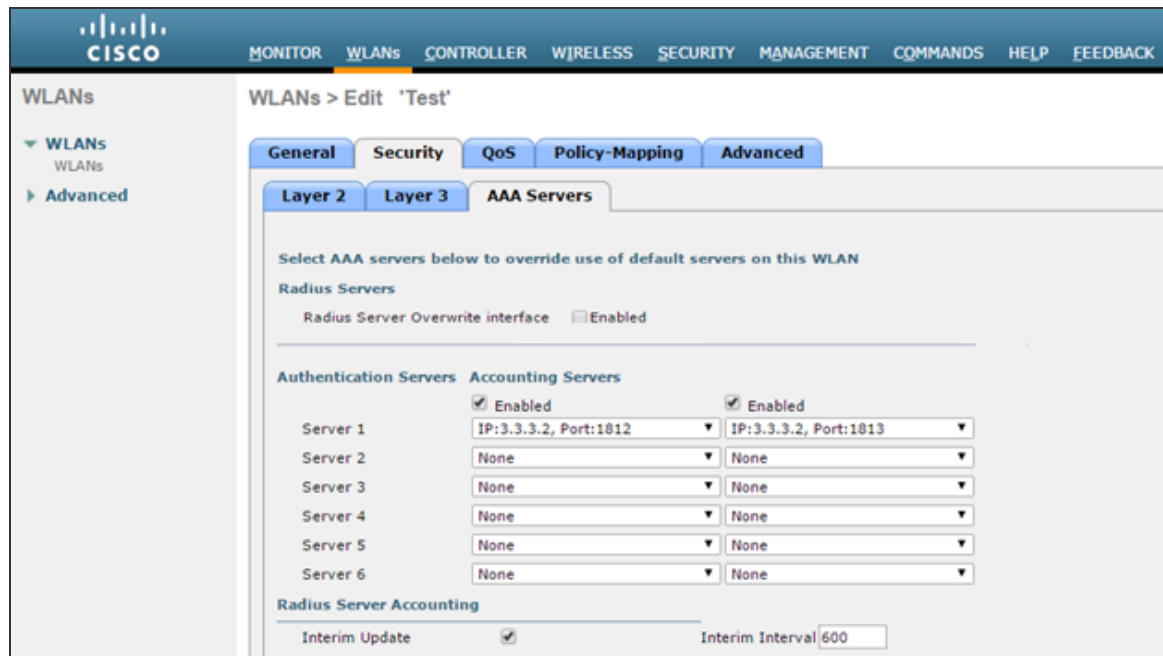
1. On the CISCO WLC main screen select WLANs tab and create a new WLAN.



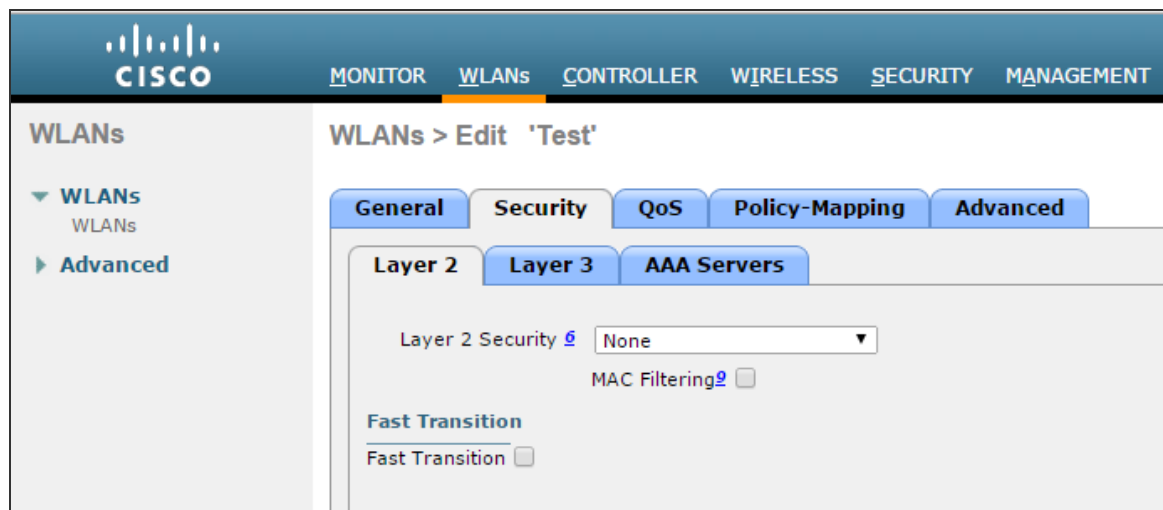
The screenshot shows the Cisco WLC interface for creating a new WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMMANDS'. The 'WLANs' tab is selected. On the left, a sidebar shows 'WLANs' and 'Advanced' options. The main area is titled 'WLANs > New' and contains the following configuration fields:

Type	WLAN
Profile Name	Test
SSID	test
ID	10

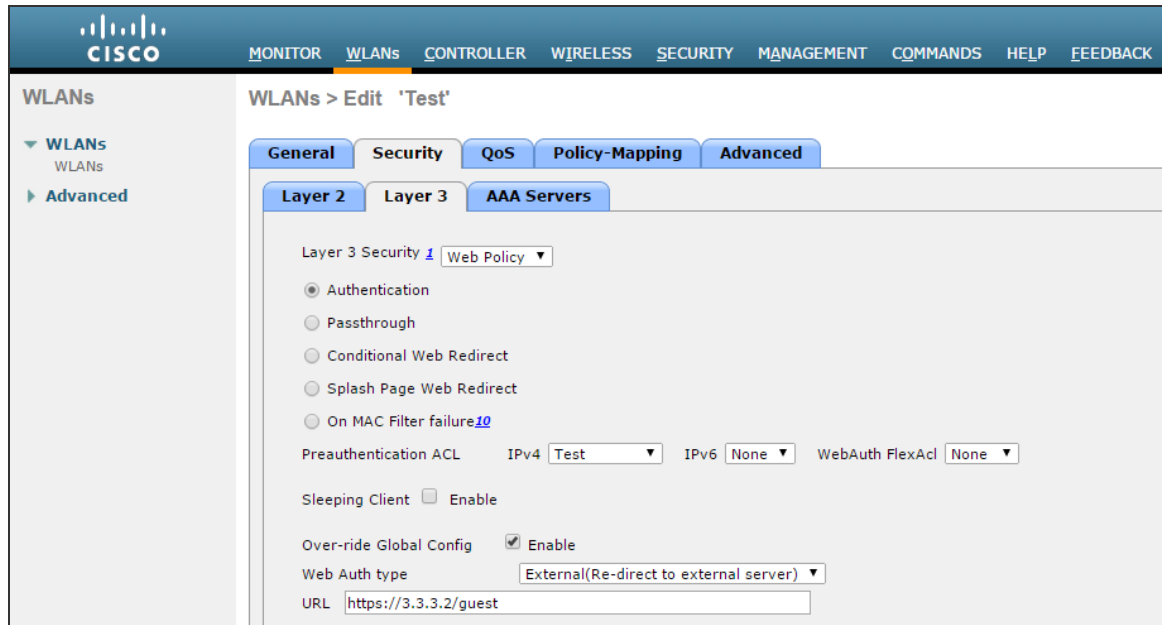
2. Select to General tab and enable Status checkbox.



3. Select Security > Layer 2 in WLANs tab. Select 'None' from the Layer 2 Security drop-down list.



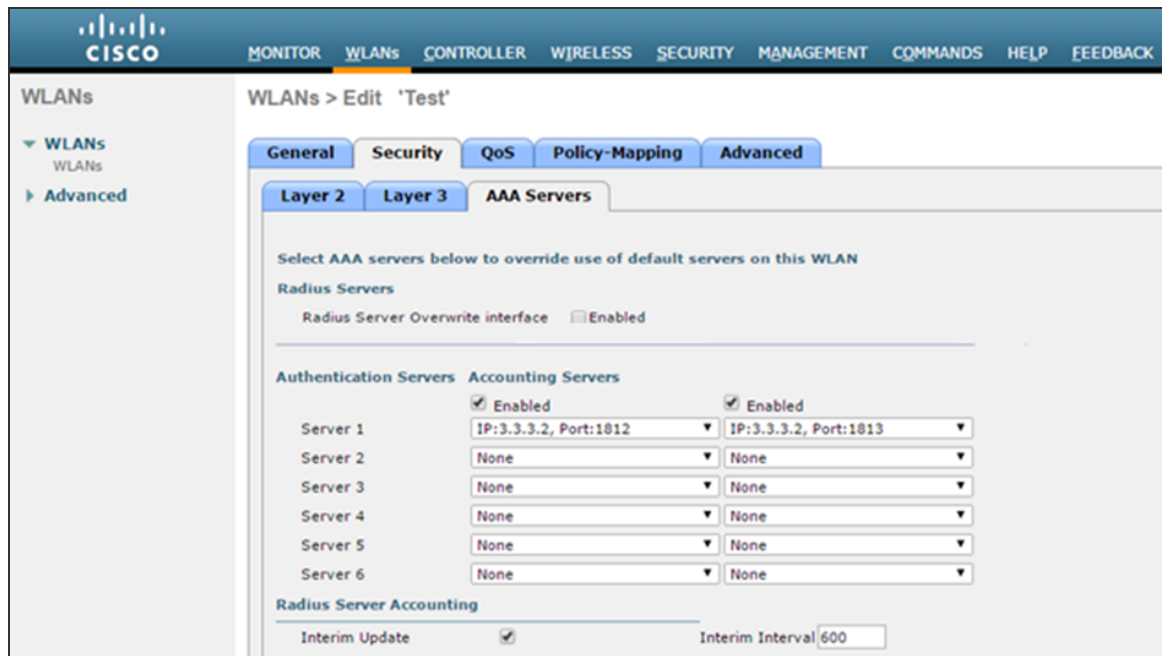
4. Select **Security > Layer3 in WLANs** tab.
 - From the Layer 3 security drop-down list select 'Web Policy'.
 - For Preauthentication ACL, associate the ACL that is created earlier for IPv4.
 - Over-ride Global Config - Select the Enable check box.
 - From the Web auth type drop-down list select External (Re-direct to external server)
 - URL – Enter the IPS (Guest sign-in URL) for redirection URL.




The screenshot displays the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > Edit 'Test'' and features tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. Under the 'Security' tab, there are sub-tabs for 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'Layer 3' sub-tab is active, showing the following configuration:

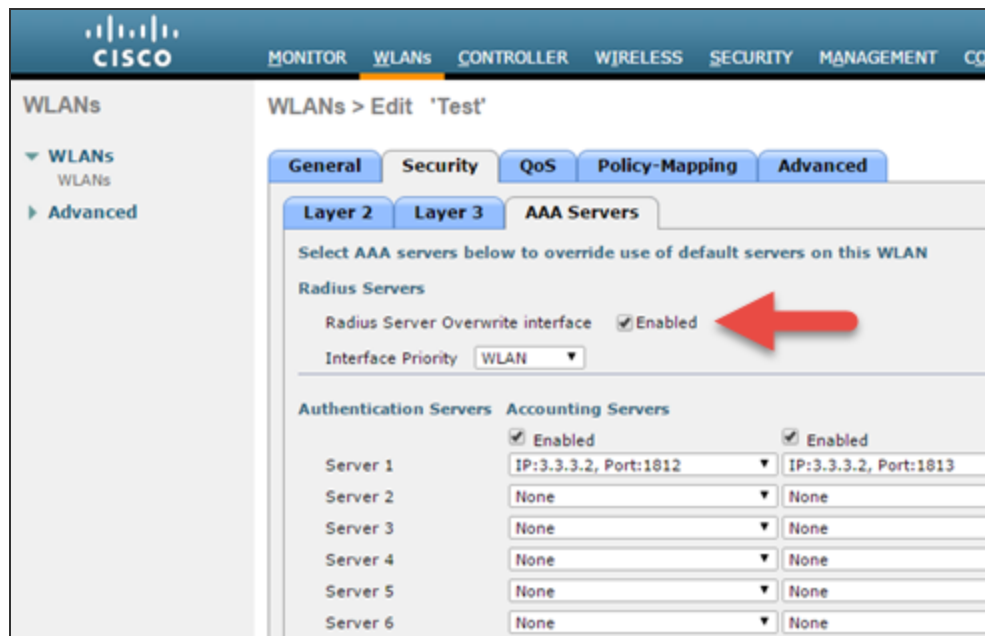
- Layer 3 Security: Web Policy (dropdown)
- Authentication: Authentication, Passthrough, Conditional Web Redirect, Splash Page Web Redirect, On MAC Filter failure
- Preauthentication ACL: IPv4: Test (dropdown), IPv6: None (dropdown), WebAuth FlexAcl: None (dropdown)
- Sleeping Client: Enable
- Over-ride Global Config: Enable
- Web Auth type: External(Re-direct to external server) (dropdown)
- URL: https://3.3.3.2/guest (text input)

5. Select **Security** > **AAA Servers** tab. Configure RADIUS server for authentication and accounting.

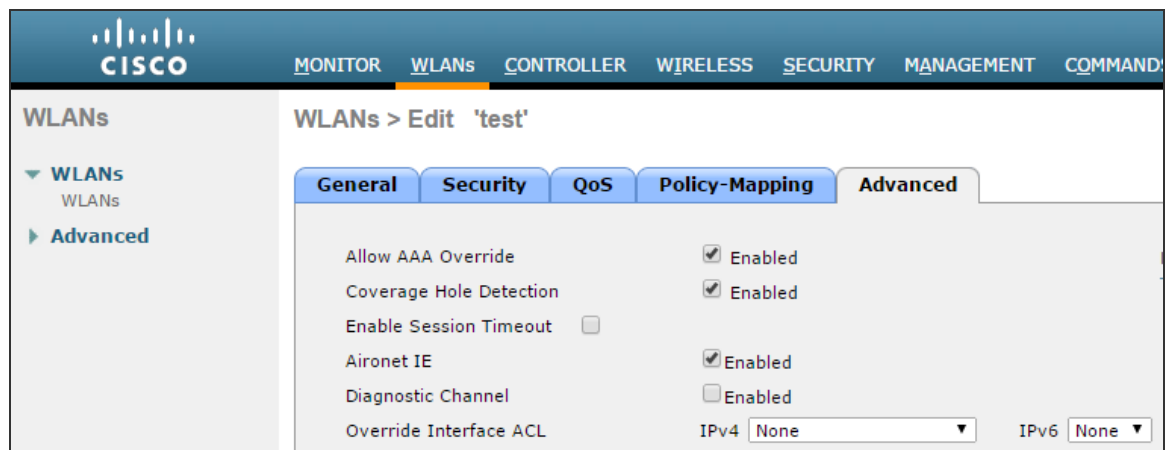


- Select the **Interim Update** check box.

 Instead of management port, if some other Interface/Interface Group (G) is selected during WLAN creation then Radius Server Overwrite interface option must be enabled.



- Select **Advanced** tab and enable Allow AAA Override checkbox.



Using CLI

Before creating a new WLAN verify the existing WLANs on the WLC using the following command and use an unused index id for the new WLAN.

```
show wlan summary
```

To create a new WLAN

```
config wlan create <WLAN_ID> <Profile name> <SSID>
```

Ex: - config wlan create 10 Test Test # Test is the WLAN name and SSID

```
config wlan interface <WLAN_ID> <interface-name>
```

Ex: - config wlan interface 10 management # assigning the WLAN to management port

```
config wlan security wpa disable <WLAN_ID>
```

```
config wlan security web-auth enable <WLAN_ID>
```

```
config wlan custom-web global disable <WLAN_ID>
```

```
config wlan custom-web ext-webauth-url <ext-webauth-url> <WLAN_ID>
```

```
config wlan custom-web webauth-type external <WLAN_ID>
```

```
config wlan security web-auth acl <WLAN_ID> <ACL_name>
```

```
config wlan radius_server auth add <WLAN_ID> <Radius_auth_server_ID>
```

```
config wlan radius_server acct add <WLAN_ID> <Radius_acct_server_ID>
```

```
config wlan radius_server overwrite-interface enable <WLAN_ID> ( This command is
required only if instead of management, some other interface is configured for WLAN.
```

Please

check steps 2 and 5)

```
config wlan radius_server acct interim-update enable <WLAN_ID>
```

```
config wlan radius_server acct interim-update <Interval> <WLAN_ID>
```

```
config wlan aaa-override enable <WLAN_ID>
```

```
config wlan enable <WLAN_ID>
```

Configuring AP Group

On the CISCO WLC main screen go to WLANs > Advanced > AP Groups screen and map WLAN to the Local AP (Campus Only mode) group.

WLAN ID	WLAN SSID ²	Interface/Interface Group(G)	SNMP NAC State
1	LWS	vlan255	Disabled <input type="checkbox"/>
2	lwsdot1x	vlan74	Disabled <input type="checkbox"/>
5	lwsnew	vlan255	Disabled <input type="checkbox"/>
6	cisco-8021x	vlan74	Disabled <input type="checkbox"/>
7	test	management	Disabled <input type="checkbox"/>

Using the CLI

```
config wlan apgroup interface-mapping add <APgroup Name> <WLAN ID> <interfacename>
```

To save the configuration use the following command:
save config

Configuration Required on Cisco WLC for Remote AP mode

Configuring RADIUS server

1. Login to Cisco WLC. Go to **Security > AAA > RADIUS**. Configure IPS server as authentication and accounting server.

2. **Support for RFC 3576** - Enable this option to trigger RADIUS disconnect when required.



Support for RFC3576 for RADIUS disconnect does not work properly with Cisco 2500, 5500, 7500, and 8500 series.

The screenshot shows the Cisco WLC GUI for configuring a new RADIUS Authentication Server. The left sidebar shows the navigation menu with 'RADIUS' expanded. The main content area is titled 'RADIUS Authentication Servers > New'. The configuration fields are as follows:

Server Index (Priority)	3
Server IP Address	3.3.3.2
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

The screenshot shows the Cisco WLC GUI for configuring a new RADIUS Accounting Server. The left sidebar shows the navigation menu with 'RADIUS' expanded. The main content area is titled 'RADIUS Accounting Servers > New'. The configuration fields are as follows:

Server Index (Priority)	7
Server IP Address	3.3.3.2
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Port Number	1813
Server Status	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

Using the CLI

Before creating the radius server, you need to allot an index number to it which is not currently in use. To find out the index numbers which are currently in use in WLC, use the following command

```
show radius summary
```

Go through the authentication servers and accounting servers section in the displayed output. Use an unused index number for adding radius authentication or accounting server.

```
config radius auth add <RADIUS auth server ID> <RADIUS server IP> 1812 ascii
<password>

config radius auth disable < RADIUS auth server ID >

config radius auth rfc3576 enable < RADIUS auth server ID >

config radius auth enable < RADIUS auth server ID >

config radius acct add <RADIUS acct server ID > <RADIUS server IP> 1813 ascii
<password>
```

Configuring FlexConnect ACLs

1. Select **Security > Access Control Lists > FlexConnect ACLS**. Create a FlexConnect ACL list to allow DNS, DHCP and IPS (Traffic).

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DHCP Server	Any	Any
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any
4	Permit	3.3.3.2 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any
5	Permit	0.0.0.0 / 0.0.0.0	3.3.3.2 / 255.255.255.255	Any	Any	Any	Any

Using the CLI

To see all the ACLs that are configured on the controller enter the following command:

```
show flexconnect acl summary
```

To create a new ACL

```
config flexconnect acl create <ACL name>
```

To create rules in the newly created ACL

```
config flexconnect acl rule add <ACL name> <Rule number1>
config flexconnect acl rule protocol <ACL name> <Rule number1> 17 # 17 is UDP
```

```
config flexconnect acl rule source port range <ACL name> <Rule number1> 68 68 # 68
is DHCP client port number
config flexconnect acl rule action <ACL name> <Rule number1> permit # Allow access

config flexconnect acl rule add <ACL Name> <Rule number2>
config flexconnect acl rule protocol <ACL name> <Rule number2> 17
config flexconnect acl rule source port range <ACL name> <Rule number2> 67 67 # 67
is DHCP server port number
config flexconnect acl rule action <ACL name> <Rule number2> permit

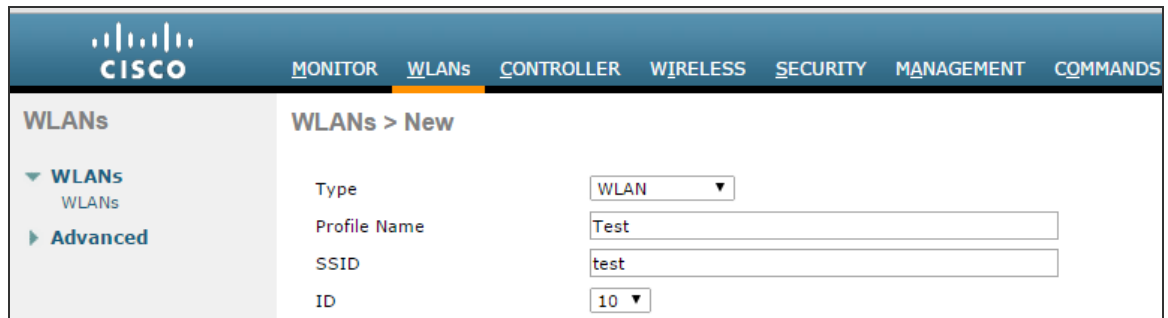
config flexconnect acl rule add <ACL name> <Rule number3>
config flexconnect acl rule protocol <ACL name> <Rule number3> 6
config flexconnect acl rule source port range <ACL name> <Rule number3> 53 53 # Port
53 for DNS
config flexconnect acl rule action <ACL name> <Rule number3> permit
config flexconnect acl rule add <ACL name> <Rule number4>
config flexconnect acl rule protocol <ACL name> <Rule number4> 6
config flexconnect acl rule destination port range <ACL name> <Rule number4> 53 53
#port 53 for DNS
config flexconnect acl rule action <ACL name> <Rule number4> permit

config flexconnect acl rule add <ACL name> <Rule number5>
config flexconnect acl rule source address <ACL name> <Rule number5> <IPS IP>
<Subnetmask>
config flexconnect acl rule action <ACL name> <Rule number5> permit

config flexconnect acl rule add <ACL name> <Rule number6>
config flexconnect acl rule destination address <ACL name> <Rule number6> <IPS IP>
<Subnetmask>
config flexconnect acl rule action <ACL name> <Rule number6> permit
```


Configuring WLAN

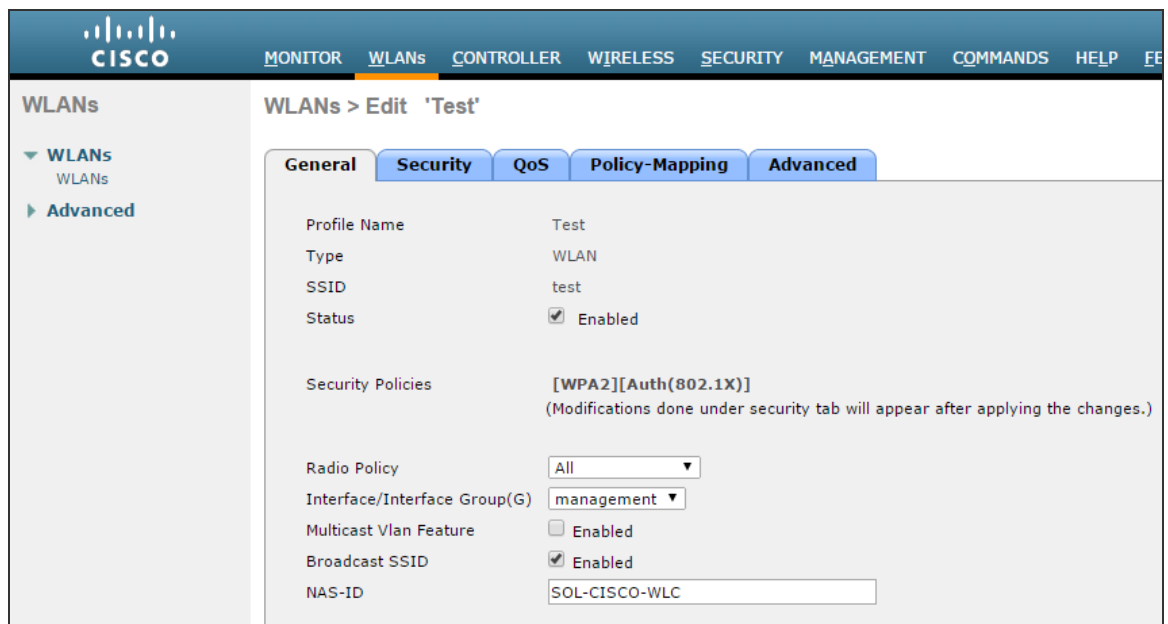
1. Go to WLANs tab and create a new WLAN.



The screenshot shows the Cisco configuration interface for creating a new WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMMANDS'. The left sidebar shows 'WLANs' with a sub-menu 'Advanced'. The main content area is titled 'WLANs > New' and contains the following fields:

Type	WLAN
Profile Name	Test
SSID	test
ID	10

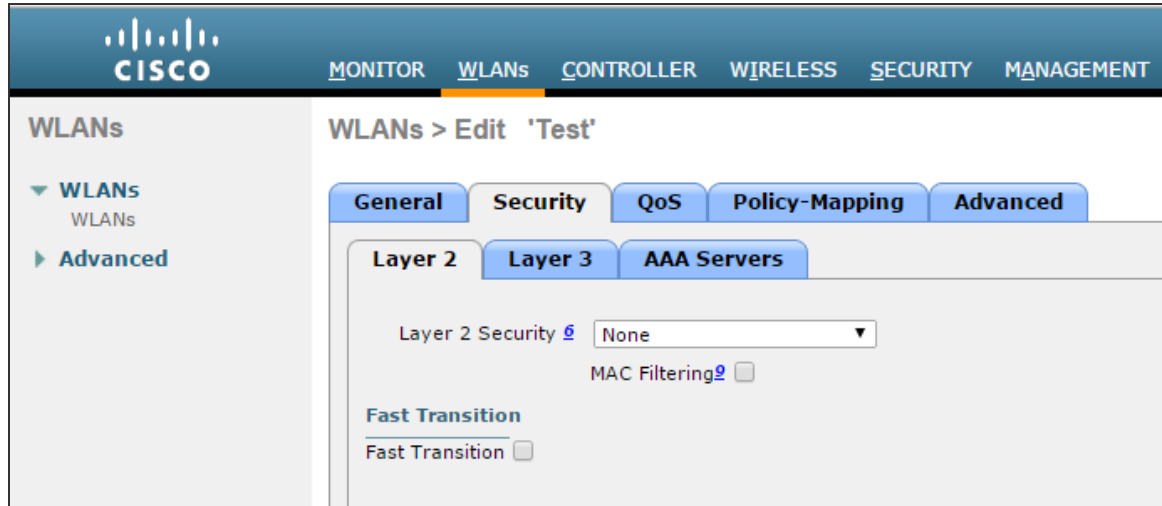
2. Navigate to General tab and enable Status checkbox.



The screenshot shows the Cisco configuration interface for editing an existing WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FE'. The left sidebar shows 'WLANs' with a sub-menu 'Advanced'. The main content area is titled 'WLANs > Edit 'Test'' and has tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'General' tab is selected, showing the following fields:

Profile Name	Test
Type	WLAN
SSID	test
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	SOL-CISCO-WLC

3. Go to Security > Layer 2 in WLAN settings. From the Layer 2 Security drop-down list Select 'None'.



The screenshot displays the Cisco WLAN configuration interface. The top navigation bar includes the Cisco logo and tabs for MONITOR, WLANs (selected), CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. The left sidebar shows the WLANs menu with sub-items for WLANs and Advanced. The main content area is titled 'WLANs > Edit 'Test'' and features several configuration tabs: General, Security (selected), QoS, Policy-Mapping, and Advanced. Under the Security tab, there are sub-tabs for Layer 2 (selected), Layer 3, and AAA Servers. The Layer 2 configuration section includes a 'Layer 2 Security' dropdown menu set to 'None', a 'MAC Filtering' checkbox which is unchecked, and a 'Fast Transition' section with an unchecked checkbox.

4. Go to Security > Layer3 in WLANs tab.
 - From the Layer 3 security drop-down list select 'Web Policy'.
 - For Preauthentication ACL, associate the FlexConnectACL that is created earlier.
 - Over-ride Global Config - Select the Enable check box.
 - From the Web auth type drop-down list select External (Re-direct to external server)
 - URL - Enter the IPS (Guest sign-in URL) for redirection URL.

The screenshot displays the Cisco WLAN configuration interface for a WLAN named 'Test'. The 'Security' tab is selected, and the 'Layer 3' sub-tab is active. The configuration includes:

- Layer 3 Security:** Set to 'Web Policy'.
- Authentication:** Selected as the primary mode.
- Preauthentication ACL:** IPv4 and IPv6 are set to 'None', and WebAuth FlexAcl is set to 'flexpreauthACL'.
- Sleeping Client:** 'Enable' checkbox is unchecked.
- Over-ride Global Config:** 'Enable' checkbox is checked.
- Web Auth type:** Set to 'External(Re-direct to external server)'.
- URL:** Set to 'https://3.3.3.2/ciscowlc'.

5. Go to **Security > AAA Servers in WLANs** tab. Configure RADIUS server for authentication and accounting.

The screenshot shows the Cisco WLAN configuration interface for a WLAN named 'Test'. The 'Security' tab is selected, and the 'AAA Servers' sub-tab is active. The interface includes a navigation menu on the left with 'WLANs' and 'Advanced' options. The main content area has tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. Under 'AAA Servers', there are sub-tabs for 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'AAA Servers' sub-tab contains the following configuration options:

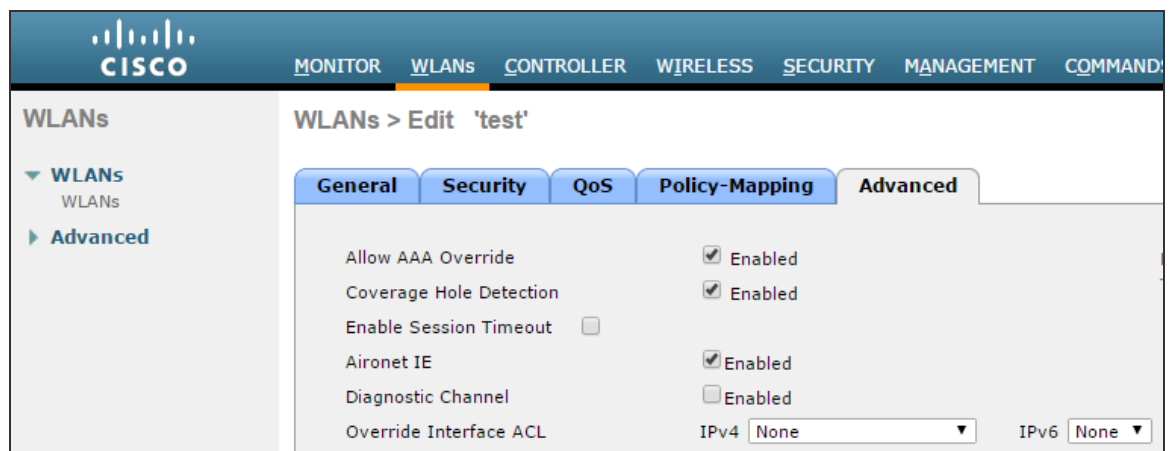
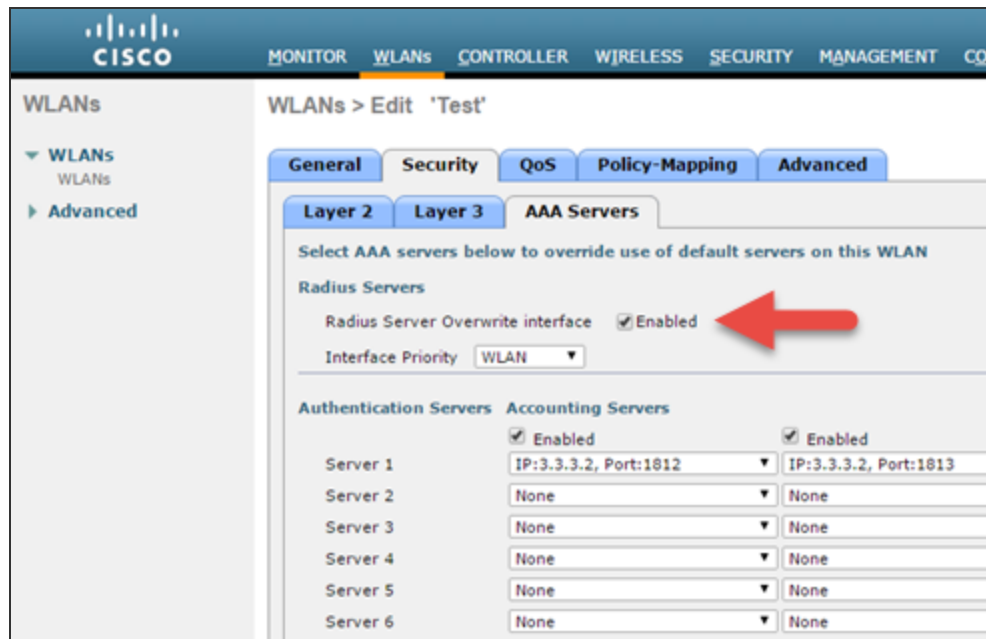
- Select AAA servers below to override use of default servers on this WLAN**
- Radius Servers**
 - Radius Server Overwrite interface Enabled
- Authentication Servers** and **Accounting Servers** (both with Enabled)
- Table of servers:

Server	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:3.3.3.2, Port:1812	<input checked="" type="checkbox"/> Enabled IP:3.3.3.2, Port:1813
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

- Radius Server Accounting**
 - Interim Update
 - Interim Interval: 600

6. Select the **Interim Update** check box.

7. Select **Advanced** tab and enable **Allow AAA Override** checkbox.



Using the CLI

Before creating a new WLAN verify the existing WLANs on the WLC using the following command and use an unused index id for the new WLAN

```
show wlan summary
```

To create a new WLAN:

```
config wlan create <WLAN_ID> <Profile name> <SSID>
eg: config wlan create 10 Test Test # Test is the WLAN name and SSID
```

```

config wlan interface <WLAN_ID> <interface-name>
eg: config wlan interface 10 management # assigning the WLAN to management port
config wlan security wpa disable <WLAN_ID>
config wlan security web-auth enable <WLAN_ID>
config wlan custom-web global disable <WLAN_ID>
config wlan custom-web ext-webauth-url <ext-webauth-url> <WLAN_ID>
config wlan custom-web webauth-type external <WLAN_ID>
config wlan security web-auth flexacl <WLAN_ID> <ACL_name>
config wlan radius_server auth add <WLAN_ID> <Radius_auth_server_ID>
config wlan radius_server acct add <WLAN_ID> <Radius_acct_server_ID>
config wlan radius_server overwrite-interface enable <WLAN_ID> ( This command is
required only if instead of management, some other interface is configured for WLAN.
Please check steps 2 and 5)
config wlan radius_server acct interim-update enable <WLAN_ID>
config wlan radius_server acct interim-update <Interval> <WLAN_ID>
config wlan aaa-override enable <WLAN_ID>
config wlan enable <WLAN_ID>

```

Configuring AP Group

1. On the CISCO WLC main screen go to **WLANs > Advanced > AP Groups** screen and map WLAN Flex AP (Remote AP mode) group.

WLAN ID	WLAN SSID ²	Interface/Interface Group(G)	SNMP NAC State
3	flex	vlan250	Disabled <input checked="" type="checkbox"/>
4	flexdot1x	vlan74	Disabled <input checked="" type="checkbox"/>
7	test	vlan250	Disabled <input checked="" type="checkbox"/>

Using the CLI

```

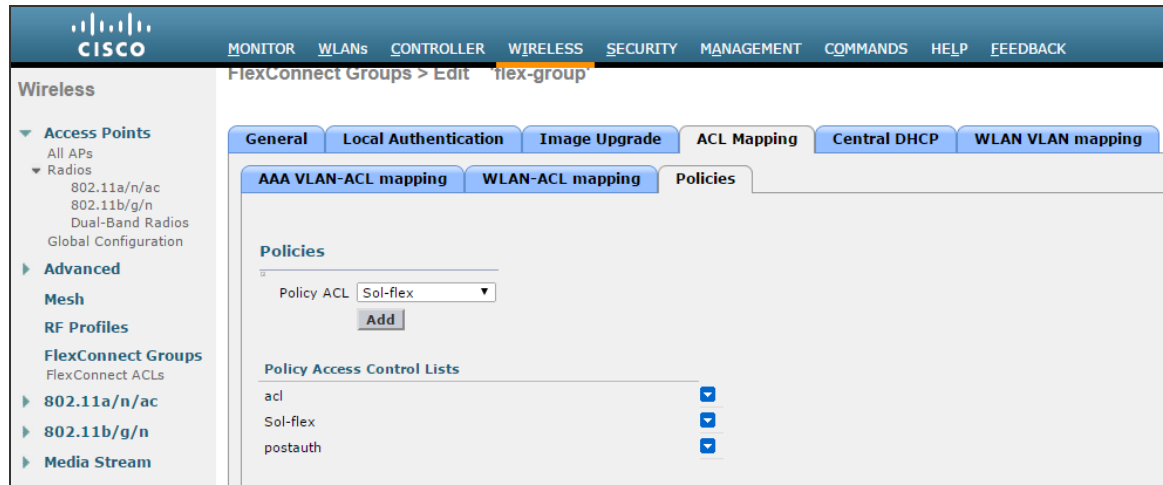
config wlan apgroup interface-mapping add <APgroup Name> <WLAN ID> <interfacename>

```

Adding ACLs in FlexConnect Group

To add ACLs in FlexConnect Group:

1. Select **Wireless > FlexConnect Groups**. Click on the required FlexConnect Group and select ACL Mapping > Policies. Add all the required FlexConnect ACLs to this group. This configuration is required when admin wants to push ACL name using RADIUS return attributes from IPS.



Using the CLI

To see all the flexconnect groups that are configured on the controller enter the following command:

```
show flexconnect group summary
```

To add policy ACLs in the flexconnect group use the following command:

```
config flexconnect group <flex-group> policy acl add <flexconnect_ACL>
```

Save the config using the following command:

```
save config
```

Configuring Cisco 3850 WLC

Configuring Cisco WLC using Web GUI

You can configure CISCO WLC 3850 by performing the steps as stated below:

1. Create a RADIUS server.
2. Create a Radius Server Group and map with the newly created RADIUS server
3. Create an Authentication list and map with the newly created Radius Server Group.

4. Create an Accounting list and map with the newly created Radius Server Group.
5. Create an Authorization list and map with the newly created Radius Server Group.
6. Create a Webauth Parameter Map
7. Create an Access List
8. Create a Sequence Number
9. Create a Wireless SSID

To configure the CISCO WLC 3850:

1. Login to CISCO WLC. The CISCO Wireless Controller home page appears.

The screenshot shows the Cisco Wireless Controller (WLC) home page. The page is divided into several sections:

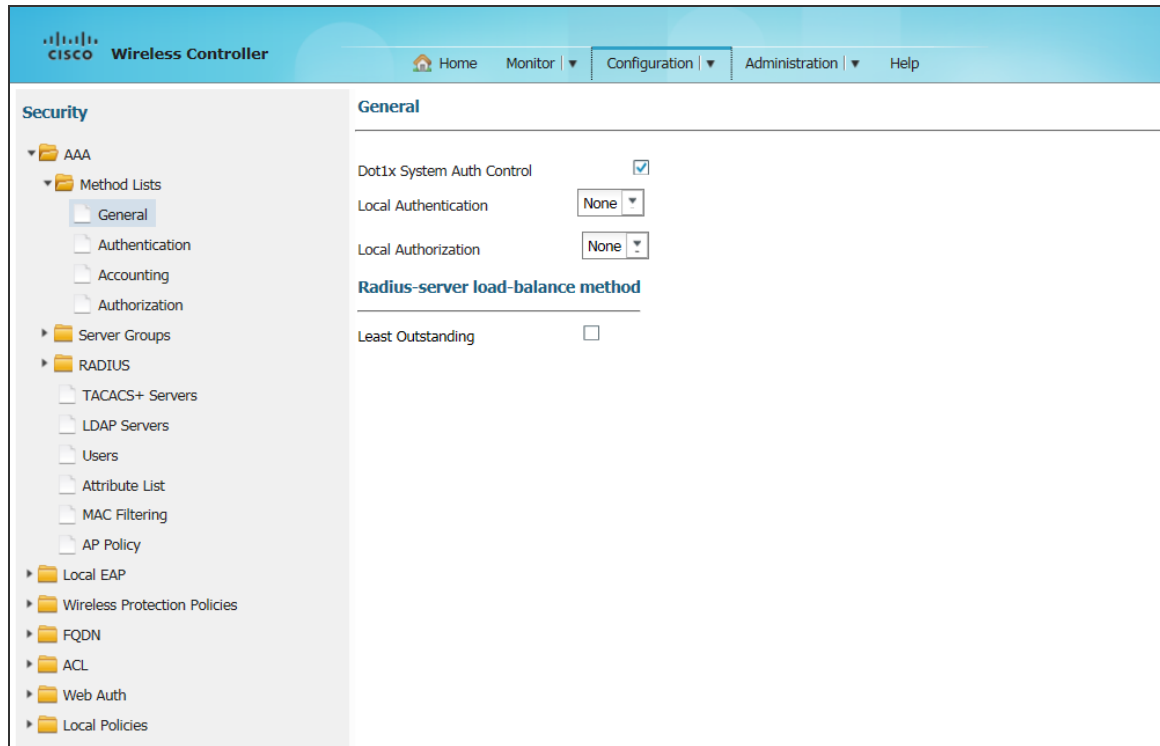
- System Summary:** Displays system time (23:26:47.949 UTC Thu Mar 5 2015), software version (03.07.00E RELEASE SOFTWARE (fc4)), system name (c3850wlc), system model (WS-C3850-24T), up time (2 weeks, 3 days, 20 hours, 0 minutes), wireless management IP (10.209.125.128), 802.11 a/n/ac Network State (Enabled), 802.11 b/g/n Network State (Enabled), mobility role (MC), and software activation (Detail).
- Access Point Summary:** A table showing the status of access points.
- Client Summary:** A section for protocol statistics, currently showing "No Protocol Statistics available".
- Search:** A search bar for username.
- Top WLANs:** A table showing the number of clients for different WLAN profiles.
- AVC for WLAN : open3850:** A section for AVC configuration, currently showing "AVC is not enabled on this WLAN".
- Rogue APs:** A table showing the number of active rogue APs, active rogue clients, and adhoc rogues.

Profile Name	Number of Clients
open3850	0
dot1x3850	0

	Total	Up	Down
802.11a/n/ac Radios	0	0	0
802.11b/g/n Radios	0	0	0
All APs	0	0	0

		Detail
Active Rogue APs	0	Detail
Active Rogue Clients	0	Detail
Adhoc Rogues	0	Detail

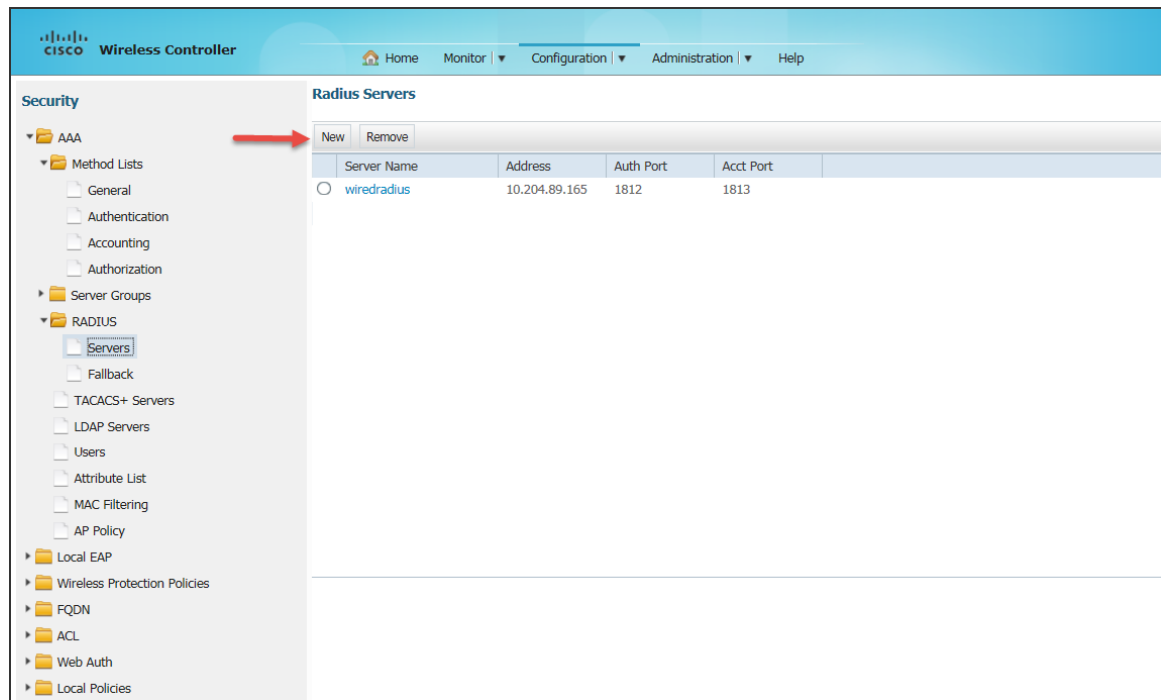
- From the **Configuration**, drop-down list select **Security**. The options under the **Security** section are displayed.



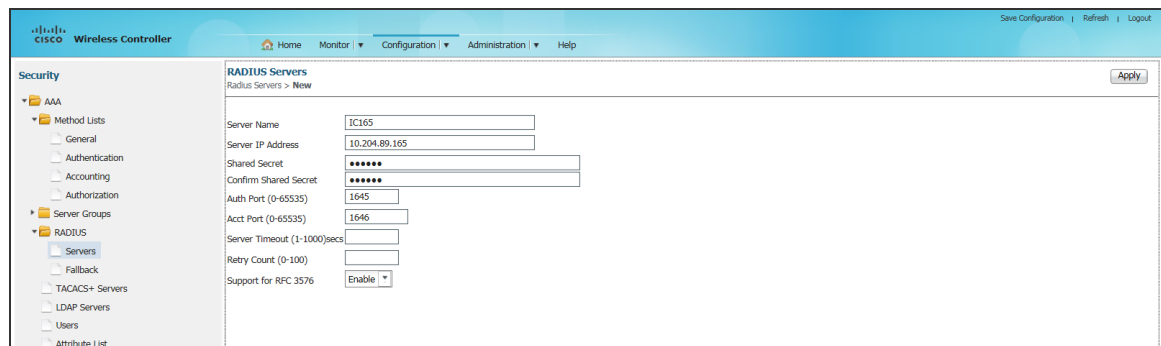
The screenshot shows the Cisco Wireless Controller configuration interface. The top navigation bar includes 'Home', 'Monitor', 'Configuration', 'Administration', and 'Help'. The left sidebar displays the 'Security' menu with various sub-items. The main content area is titled 'General' and contains the following settings:

- Dot1x System Auth Control:
- Local Authentication:
- Local Authorization:
- Radius-server load-balance method**
- Least Outstanding:

3. Select **AAA > Radius > Servers** to create a Radius server. The Radius Server screen appears.

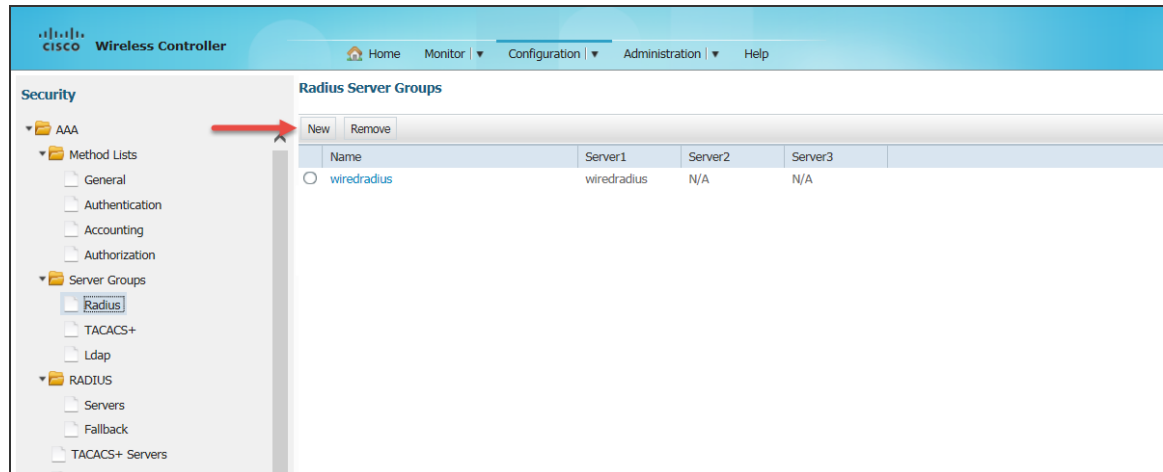


4. Click **New** to create a Radius server.

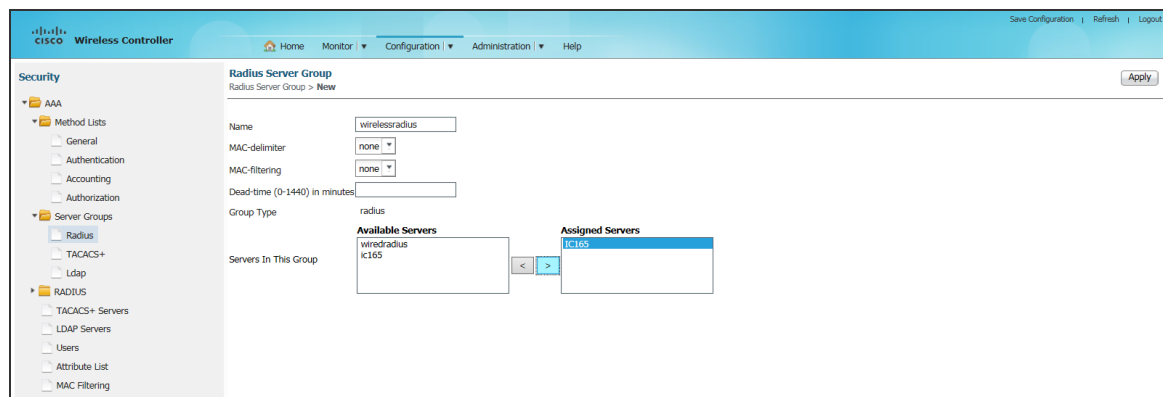



5. Enter relevant details and click Apply at the right top corner of the page. A new RADIUS server is created.

6. Select **AAA > Server Groups > RADIUS** to create a Radius Server Group. The Radius Server Groups screen appears.

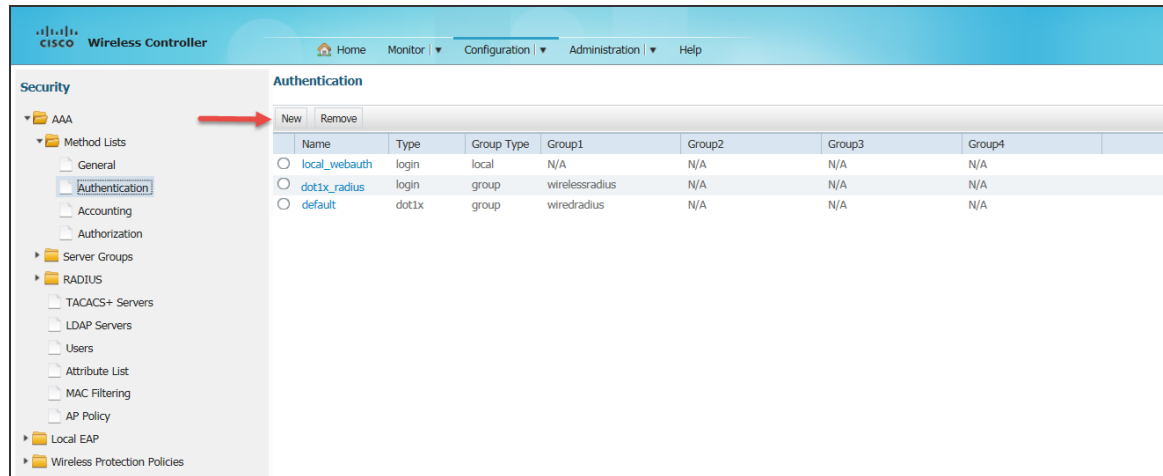


7. Click **New the Radius Server Group > New** screen appears.

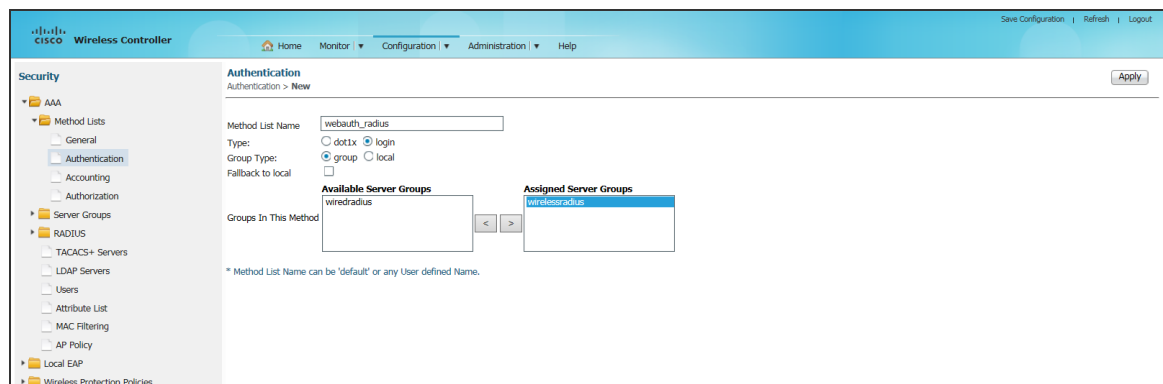


8. Enter a name in the Name field. From the Available Servers box select the server which you have created in step 5 and click the button  to move it to the Assigned Servers box.
9. Click Apply to save the Radius Server Group.


10. Select **AAA > Method List > Authentication** to create an Authentication list.
The Authentication screen appears.



11. Click **New**. The **Authentication > New** screen appears.

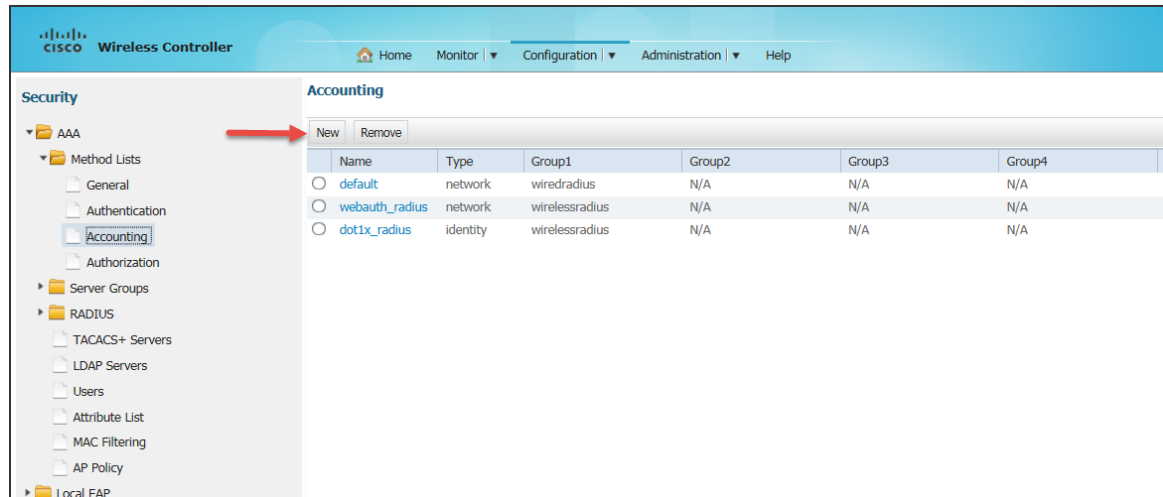


12. Enter the details in the fields as follows:

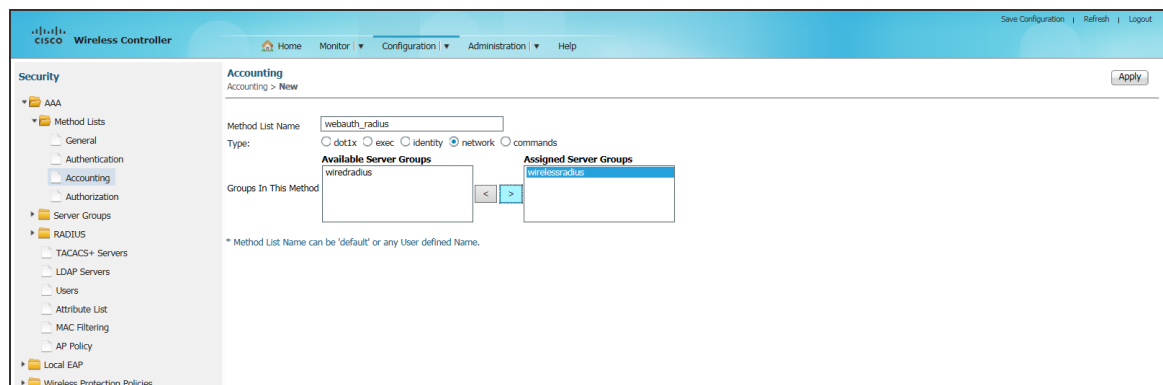
- In the Method List Name field enter webauth_radius
- For Type, select login
- For Group Type select group
- Select the 'wirelessradius' server group that you have created earlier from the Available Server Groups box and click  to move it to the Assigned Server Groups box.

13. Click **Apply** to save the Authentication.


14. Select **AAA > Method List > Accounting** to create an Accounting list. The Accounting screen appears.



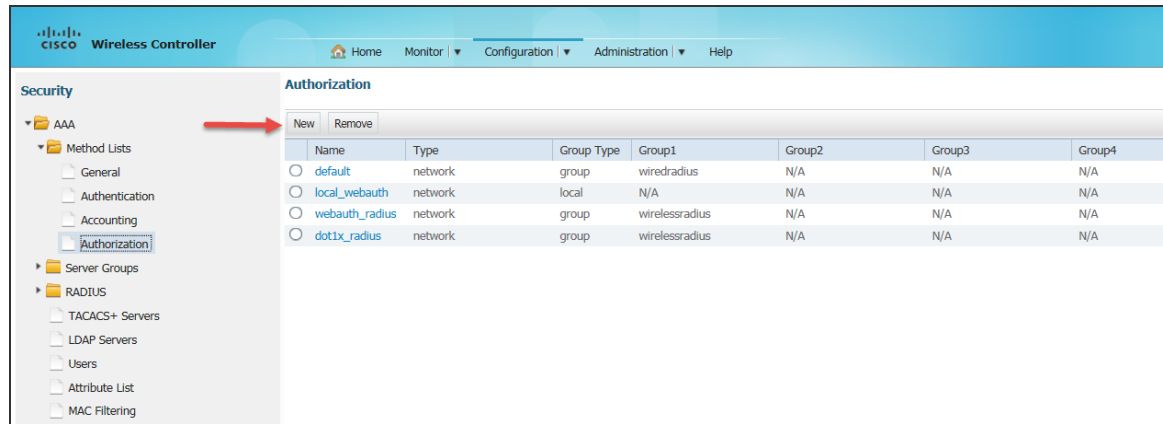
15. Click **New** to create an Accounting list. The **Accounting > New** screen appears.



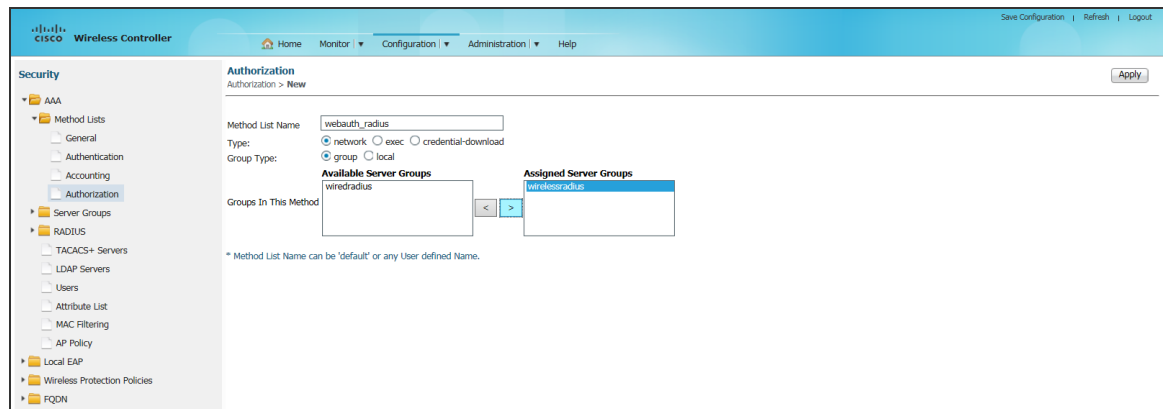
16. Enter the details in the fields as follows:

- In the Method List Name field enter webauth_radius.
- For Type, select network.
- Select the 'wirelessradius' server group that you have created earlier from the Available Server Groups box and click  to move it to the Assigned Server Groups box.
- Click Apply to save the Accounting list.


17. Select **AAA > Method Lists > Authorization** to create an Authorization list. The Authorization screen appears.



18. Click **New** to create an Authorization list. The **New** screen appears.

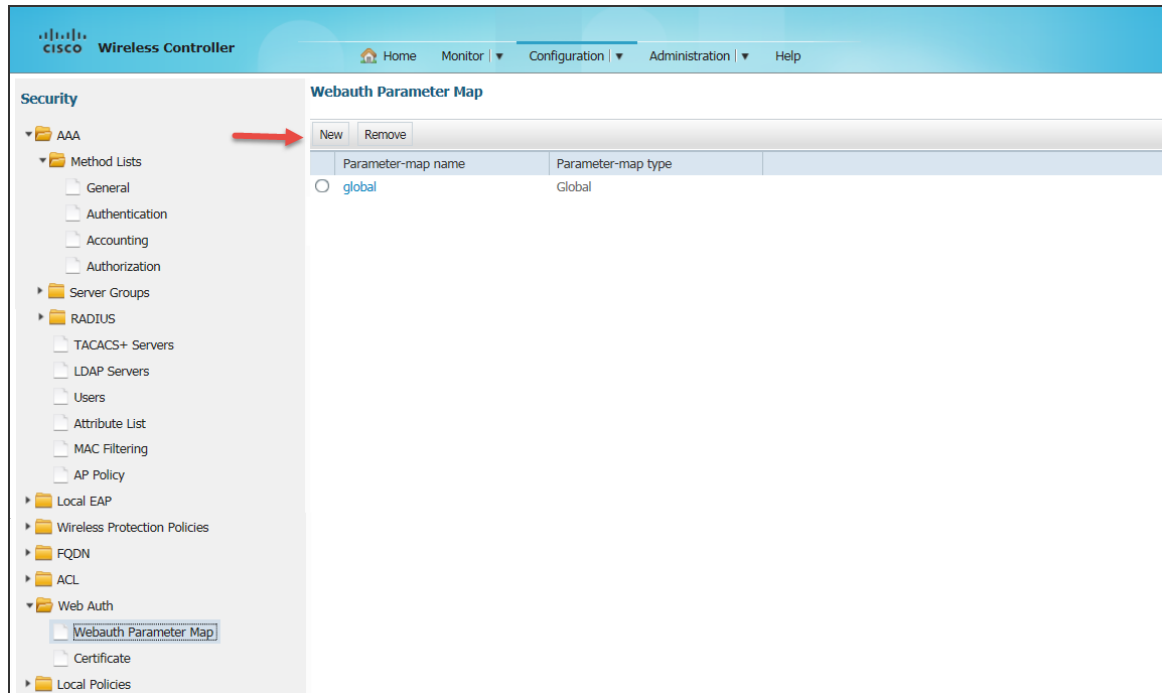


19. Enter the details in the fields as follows:

- In the Method List Name field enter webauth_radius.
- For Type, select network.
- For Group Type select group.
- Select the 'wirelessradius' server group that you have created earlier from the Available Server Groups box and click  to move it to the Assigned Server Groups box.

20. Click Apply to save the Authorization list.

21. Select Web Auth > Webauth Parameter Map to create a Webauth Parameter Map. The Webauth Parameter Map screen appears.



The screenshot shows the Cisco Wireless Controller interface. The left sidebar is titled "Security" and contains a tree view of configuration categories. The "Web Auth" category is expanded, and "Webauth Parameter Map" is selected. A red arrow points from the "Webauth Parameter Map" item in the sidebar to the "New" button in the main content area. The main content area is titled "Webauth Parameter Map" and contains a table with the following data:

Parameter-map name	Parameter-map type
<input type="radio"/> global	Global

22. Click **New** to create a Webauth Parameter Map. The **Webauth Parameter Map > New** screen appears.

The screenshot shows the Cisco Wireless Controller configuration interface for a new Webauth Parameter Map. The left sidebar shows the navigation tree with 'Webauth Parameter Map' selected under 'Web Auth'. The main configuration area is titled 'Webauth Parameter Map > New' and contains the following fields:

- Parameter-map name: vt_web
- Banner: (empty text box)
- Maximum HTTP connections(1-200): 30
- Init-State Timeout (60-3932100 in seconds): 120
- Fin-Wait Timeout (1-2147483647 in millisecond): 3000
- Type: webauth
- Turn-on Consent with Email: (checkbox, unchecked)
- Sleeping Client**
- Status: (checkbox, unchecked)
- Timeout (60-2147483647 in minutes): (empty text box)
- Customized page**
- Failed authentication proxy: --Select--
- Auth-proxy login parameters: --Select--
- Expired authentication proxy: --Select--
- Successful authentication proxy: --Select--
- Redirect to external server**
- Redirect for login: https://10.204.89.165/
- Redirect On-Failure: (empty text box)
- Redirect On-Success: (empty text box)
- Portal IPv4 address: 10.204.89.165
- Portal IPv6 address: (empty text box)

23. Enter the details in the fields as follows:

- In the Parameter – map name field enter vt_web.
- In Maximum HTTP connections (1-200) enter 30.
- In Init-State Timeout (60-3932100 in seconds) enter 120.
- In Fin-Wait Timeout (1-2147483647 in millisecond) enter 3000.
- In Redirect for login field enter https://10.204.89.165/guest - This is the IPS URL to which a guest is redirected when tried to access a website.
- In Portal IPv4 address enter 10.204.89.165.

24. Click **Apply** to save the Webauth Parameter Map.

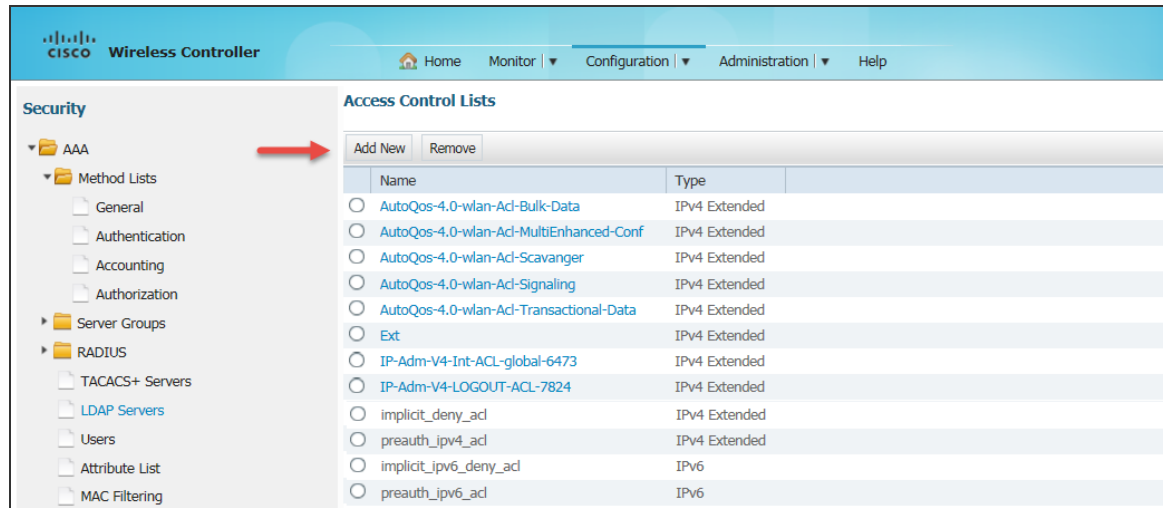


A default Webauth Parameter Map is created as shown in the following figure.

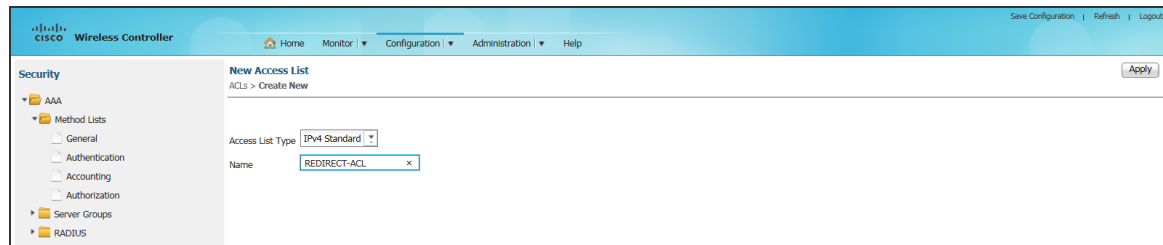
The screenshot displays the Cisco Wireless Controller configuration interface for a Webauth Parameter Map. The left sidebar shows the navigation tree under 'Security' > 'Web Auth' > 'Webauth Parameter Map'. The main content area is titled 'Webauth Parameter Map' and 'Webauth Parameter Map > Edit'. The configuration is organized into several sections:

- Parameter-map name:** global
- Banner:** (Empty text area)
- Maximum HTTP connections(1-200):** 30
- Init-State Timeout (60-3932100 in seconds):** 120
- Fin-Wait Timeout (1-2147483647 in millisecond):** 3000
- Type:** webauth
- Turn-on Consent with Email:**
- Virtual IPv4 Address:** 1.1.1.1
- Virtual IPv4 hostname:** (Empty text box)
- Virtual IPv6 Address:** (Empty text box)
- Virtual IPv6 hostname:** (Empty text box)
- Webauth intercept HTTPs:**
- Sleeping-Client:**
 - Status:** Enabled
 - Timeout (60-2147483647 in minutes):** (Empty text box)
- Customized page:**
 - Failed authentication proxy:** --Select--
 - Auth-proxy login parameters:** --Select--
 - Expired authentication proxy:** --Select--
 - Successful authentication proxy:** --Select--
- Redirect to external server:**
 - Redirect for login:** (Empty text box)
 - Redirect On-Failure:** (Empty text box)
 - Redirect On-Success:** (Empty text box)
 - Portal IPv4 address:** (Empty text box)
 - Portal IPv6 address:** (Empty text box)

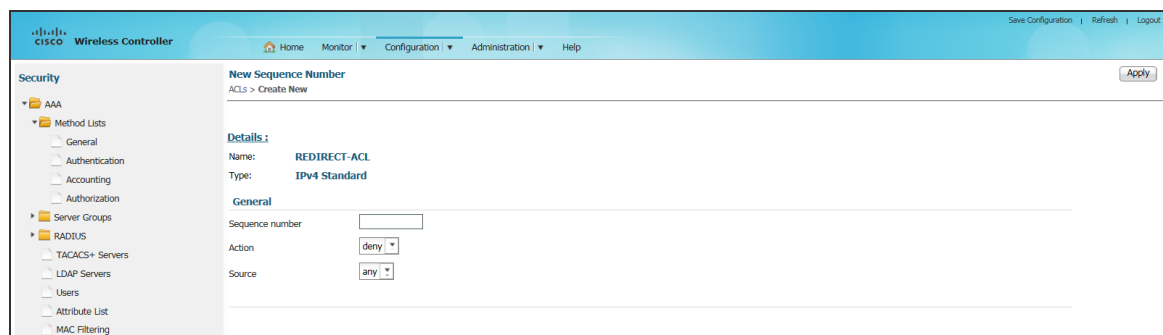
25. Select **ACL > Access Control List** to create an Access Control List. The Access Control Lists screen appears.



26. Click **Add New**. The New Access List screen appears.



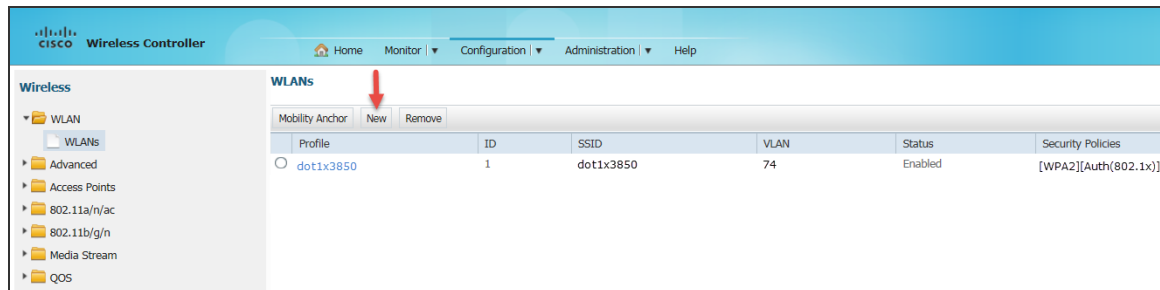
27. In the Name field enter **REDIRECT-ACL**, and then click **Apply** at the right top corner. The **New Sequence Number** screen appears.



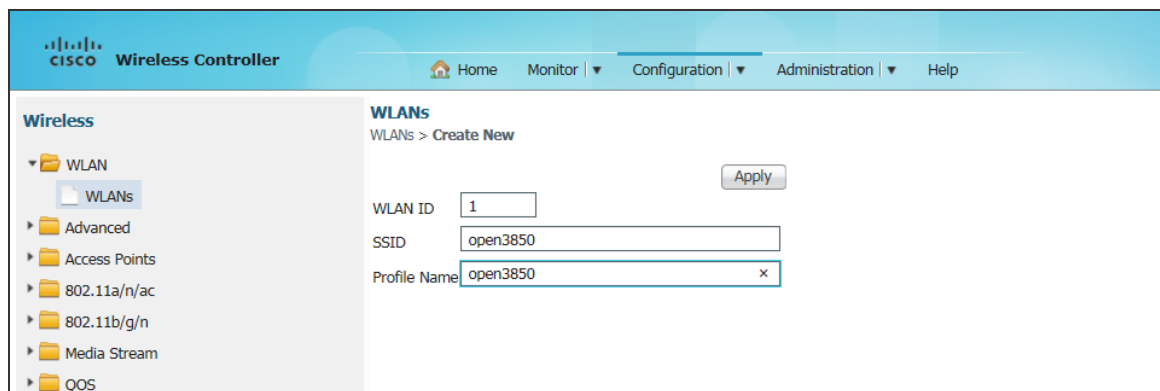
- Enter relevant details and click **Apply**. Allow traffic to the Ivanti Policy server IP address - 10.204.89.165.



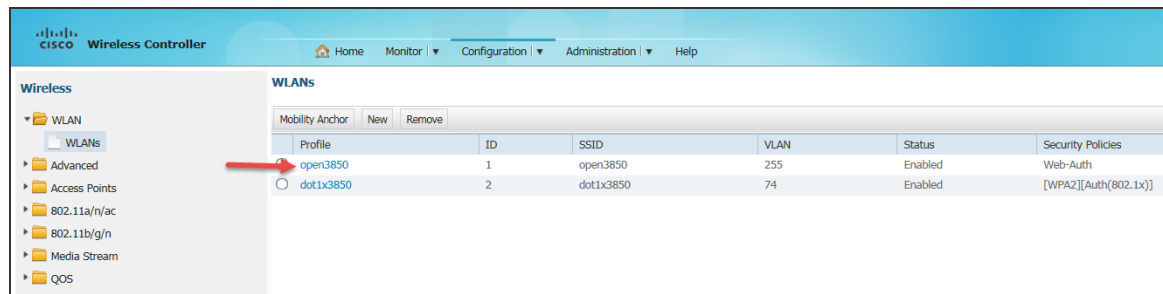
- On the main menu select **Configuration > Wireless to create a Wireless SSID**. The WLANs screen appears.



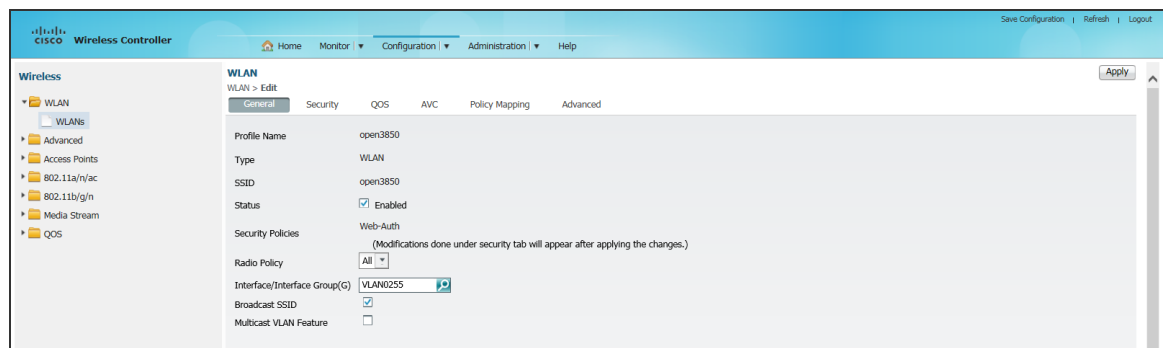
- Click **New**. The **WLANs > Create New** screen appears.



31. Click **Apply**. The WLAN is created and displayed in WLANs screen.

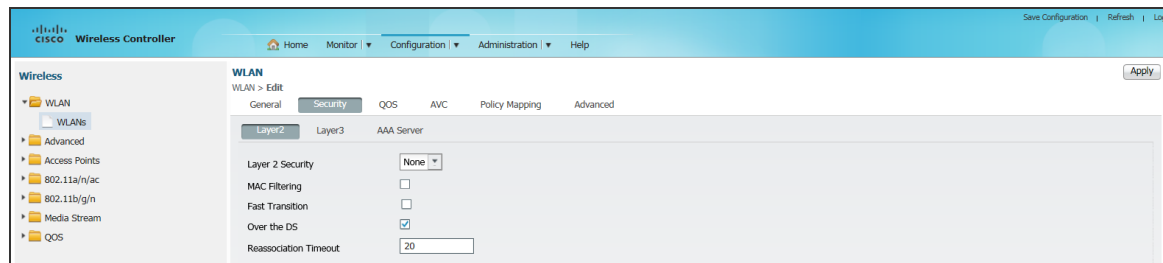


32. Click the WLAN to configure. The General tab options of the WLAN appears.



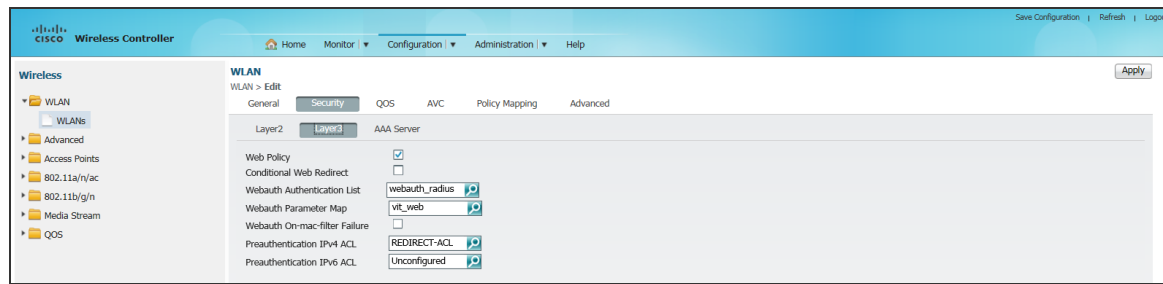
33. Select the options as shown in figure and then click **Apply** to save the configurations.

34. Click the **Security** tab. The options under **Security > Layer2** appears.



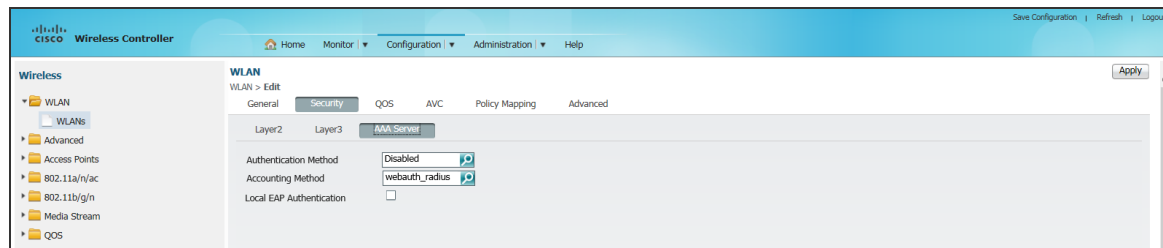
35. Select the options as shown in figure and then click Apply to save the configurations.

36. Click **Layer3** The options under Layer3 appears.



37. Select the options:
38. For Webauth Authentication List select 'webauth_radius' which you have created earlier.
39. For Preauthentication IPv4 ACL select 'REDIRECT-ACL' which you have created earlier.
40. Click Apply to save the configurations.
41. Click **AAA Server**.

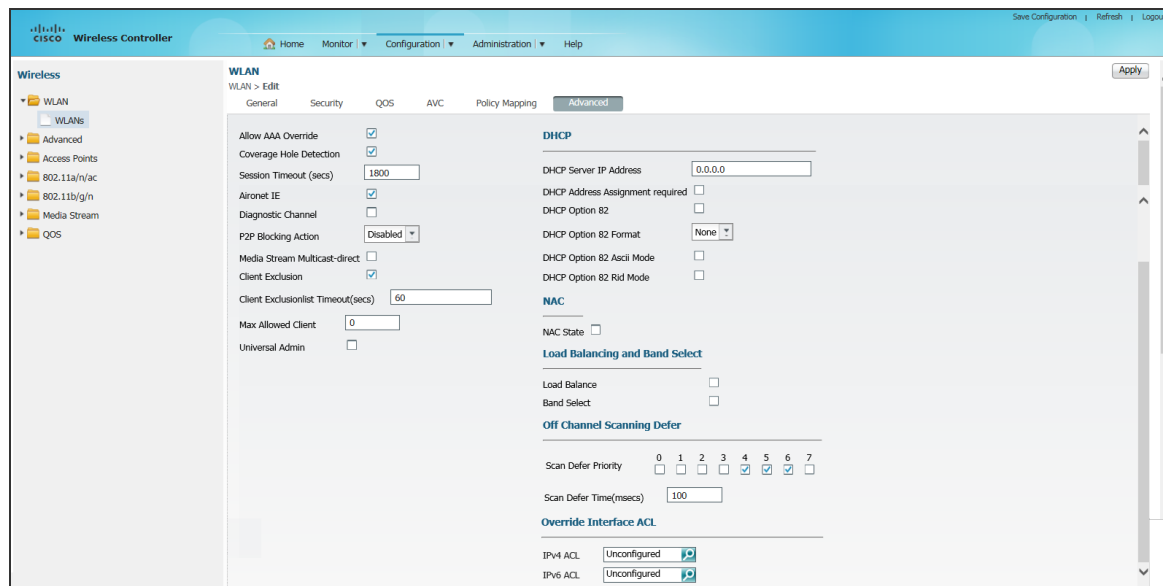
The options under AAA Server appears.



42. From the Accounting Method drop-down list select 'webauth_radius' which you have created earlier. Click **Apply** to save the configurations.

43. Click **Advanced**.

The options under Advanced appears.



44. Select the check box Allow AAA Override, so that radius attribute sent from IPS can be applied. Select other options as shown in the above figure and then click Apply to save the configurations.

Configuring Cisco WLC using CLI

Configuring RADIUS server

```
radius server <RADIUS-Profile-Name>
address ipv4 <RADIUS-Server-IP> auth-port <auth-port> acct-port <acct-port>
key <RADIUS-Shared-Secret>
```

Configuring server group

```
aaa group server radius <Server-group-name>
server name <RADIUS-Server-name>
```

Configuring AAA method lists

```
aaa authentication login <authentication-list-name> group <Server-group-name>
aaa authorization network <authorization-list-name> group <Server-group-name>
```

```
aaa accounting network <accounting-list-name>action-type start-stop group <Server-  
group-name>
```

Configuring Webauth Parameter-map

```
parameter-map type webauth <Webauth-name>  
type webauth  
redirect for-login <IPS-guest-URL>  
redirect portal ipv4 <IPS-IP>
```

Configuring IPv4 extended ACL

```
ip access-list extended <ACL-Name>  
permit ip any host <IPS-IP>  
permit ip host <IPS-IP> any  
permit udp any eq domain any  
deny ip any any
```

Configuring WLAN profile

```
wlan <wlan-profile-name> <wlan-id> <ssid-name>  
aaa-override  
accounting-list <accountung-list-name>  
client vlan <vlan-id>  
ip access-group web <ipv4-acl>  
no security wpa  
security web-auth  
security web-auth authentication-list <authentication-list-name>  
security web-auth parameter-map <parameter-map name>  
no shutdown
```

Configuring Cisco 2620 for Guest Wired Authentication

```
policy-map type control subscriber POLICY_Gil/0/24  
event session-started match-all  
10 class always do-until-failure  
10 authenticate using mab priority 10  
event authentication-failure match-first  
5 class DOT1X_FAILED do-until-failure  
10 terminate dot1x  
20 authentication-restart 60
```

```
10 class MAB_FAILED do-until-failure
10 terminate mab
    20 authenticate using dot1x priority 20
        20 class DOT1X_NO_RESP do-until-failure
            10 terminate dot1x
            20 authentication-restart 60
40 class always do-until-failure
    10 terminate mab
    20 terminate dot1x
    30 authentication-restart 60
event agent-found match-all
10 class DOT1X_MEDIUM_PRIO do-until-failure
    10 authenticate using dot1x priority 20
event authentication-success match-all
10 class always do-until-failure
    10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
```

Configuring Interface

```
switchport mode access
authentication periodic
authentication timer reauthenticate server
access-session host-mode multi-domain
access-session port-control auto
no snmp trap link-status
dot1x pae authenticator
spanning-tree portfast
service-policy type control subscriber POLICY_Gil/0/24
```

Configuring ACLs

```
C2960X(config)#ip access-list extended as-redirect    (Configure the same on IPS Radius
Return Attributes)
C2960X(config-ext-nacl)#deny ip any host 10.xxx.xx.xxx    (IPS IP)

C2960X(config-ext-nacl)#permit ip any any
C2960X(config-ext-nacl)#do wr mem
```

Configuring RADIUS CoA

```
under aaa server radius dynamic-author :
```



```
client 10.xxx.xx.xxx server-key xxx . Save
radius server test
  address ipv4 10.xxx.xx.xxx auth-port 1645 acct-port 1646
  key r
C2960X(config)#aaa group server radius dsad-IPV6
C2960X(config-sg-radius)#server name test
/**Go to interface : type mab and save**/
C2960X(config)#interface GigabitEthernet 1/0/14
      C2960X(config-if)#mab
```

Configuring Aruba WLC

Configuring Aruba WLC for IPS Guest Self-Registration

This sections explains the steps to configure Aruba WLC for deploying IPS GUAM and 'Guest Self-Registration' feature. This section provides examples of how to configure the Aruba WLC. For more information, see Aruba documentation.

Configuration required on Aruba WLC for Campus Only mode

WLAN Configuration for Campus Only mode

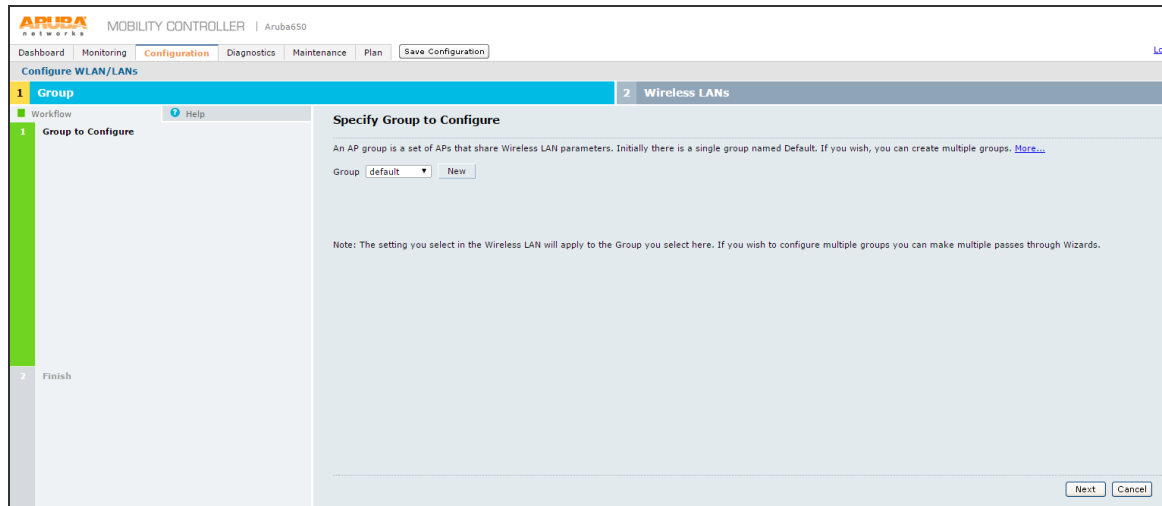
1. Log in to **Aruba WLC**. Select **Configuration > Wizards > WLAN/LAN Wizard**. The Welcome to the WLAN/LAN Configuration Wizard appears.

The screenshot displays the Aruba Mobility Controller web interface. At the top, the header shows the Aruba Networks logo, 'MOBILITY CONTROLLER | Aruba650', and a navigation menu with tabs for Dashboard, Monitoring, Configuration (selected), Diagnostics, Maintenance, and Plan. A 'Save Configuration' button is visible in the top right. Below the navigation, the page title is 'Configure WLAN/LANs'. The main content area is titled 'Welcome to the WLAN/LAN Configuration Wizard' and presents two deployment scenarios:

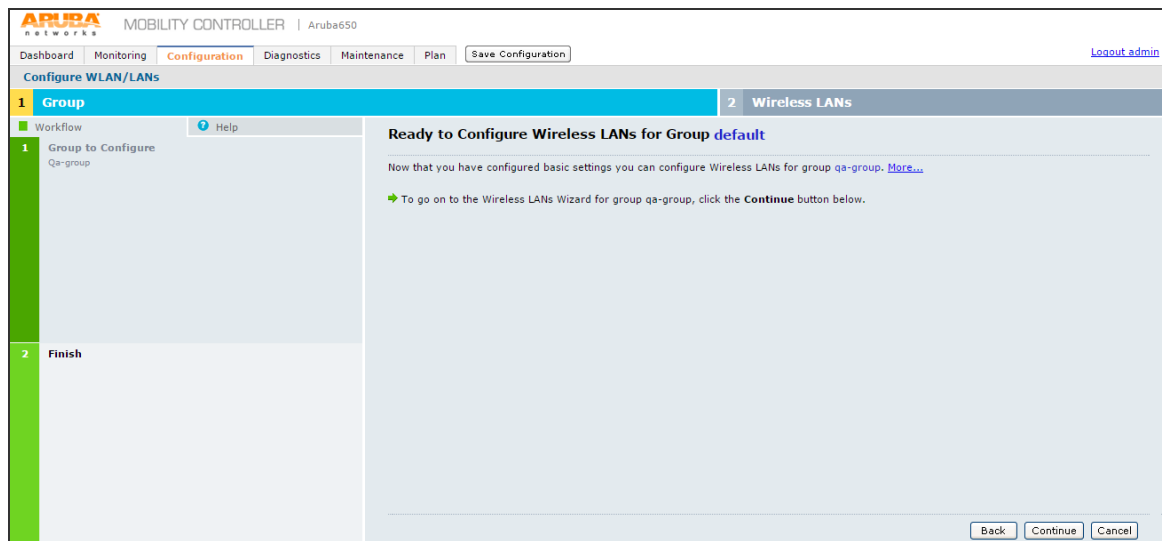
- Campus Only -- all of the access points will be physically connected to the local controller
- Remote Networking -- some of the access points will be deployed at remote locations

A diagram titled 'Campus Wireless' illustrates a central Mobility Controller connected to several access points (APs) distributed across a campus floor plan. The interface concludes with 'Begin' and 'Cancel' buttons.

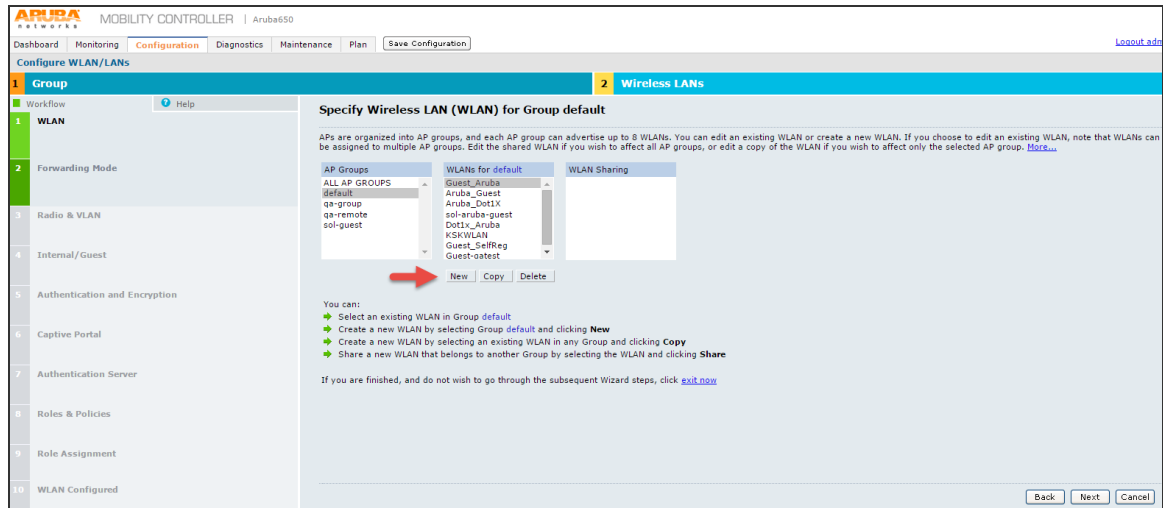
2. Select **Campus Only** option and click **Begin**. The Specify Group to Configure screen appears.



3. On Specify Group to Configure screen select an existing AP group or create a new AP group and click **Next**. The Ready to Configure Wireless LANs for Group screen appears.

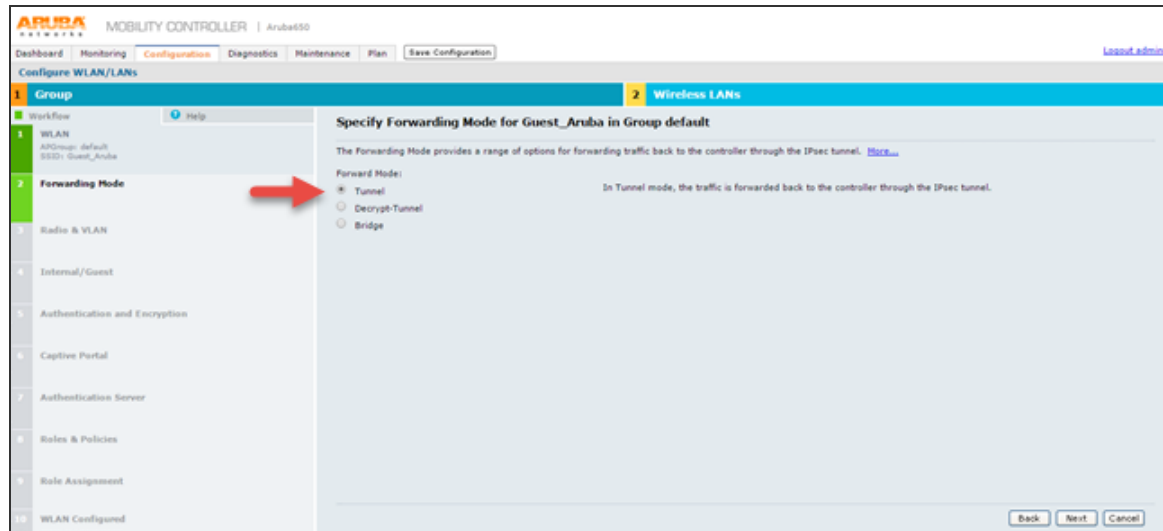


- Click **Continue** button. The Specify Wireless LAN (WLAN) for Group default screen appears.

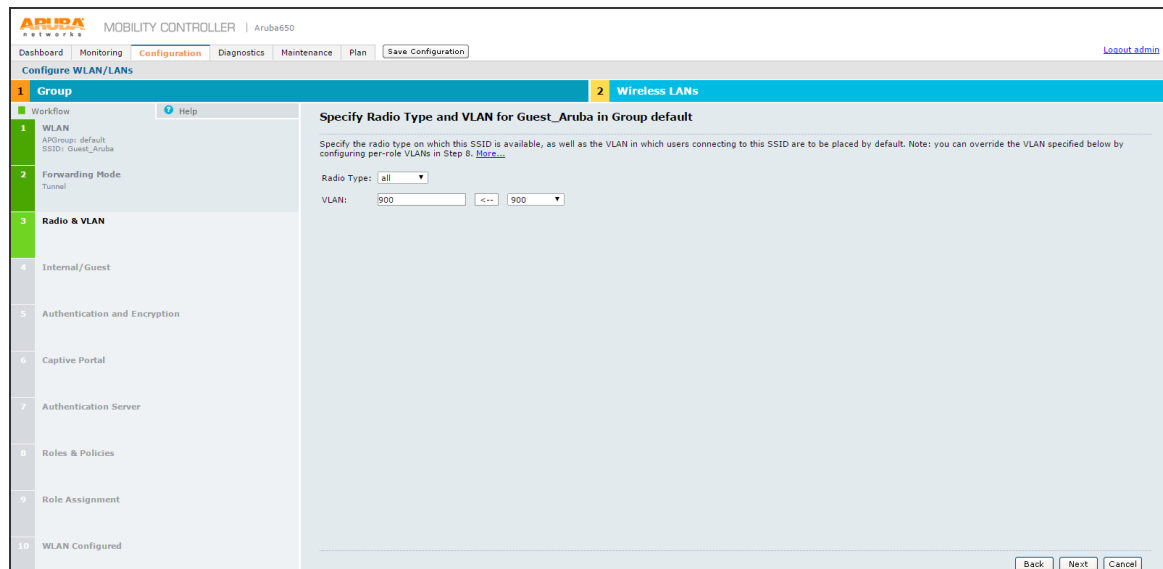


- On Specify Wireless LAN (WLAN) for Group default screen, select a group from the AP Groups list.
- In the WLANS for list do one of the following:
 - Select an existing WLAN.
 - Click **New** to create a new WLAN.
- Click **Next**.

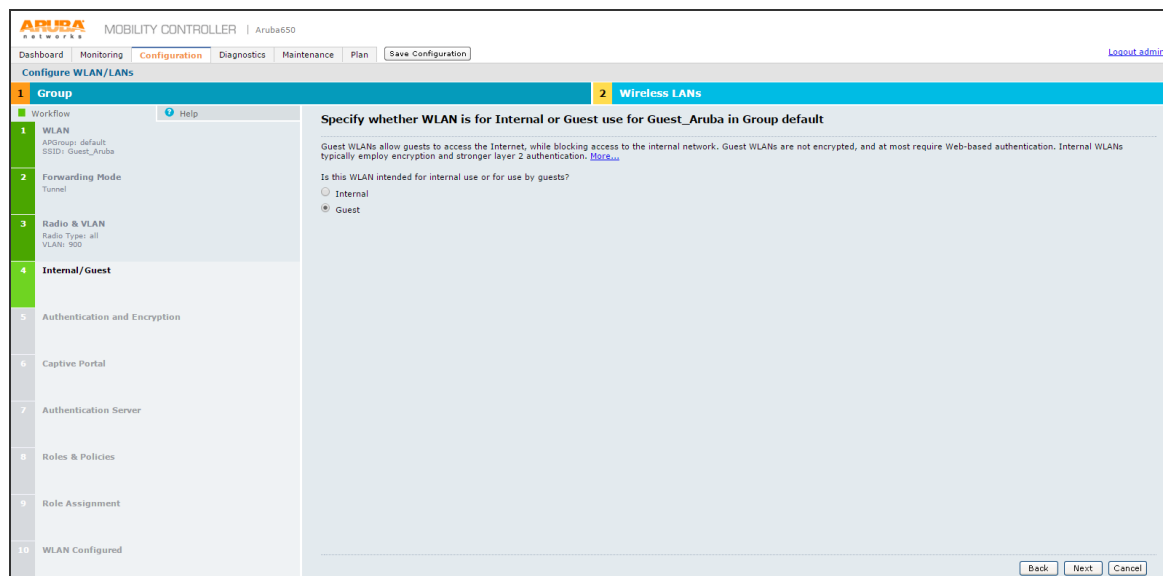
- The Specify Forwarding Mode for Guest_Aruba in Group default screen appears.



- On Specify Forwarding Mode for Guest_Aruba in Group default screen, under Forward Mode, select Tunnel option and click **Next**. The Specify Radio Type and VLAN for Guest_Aruba in Group default screen appears.

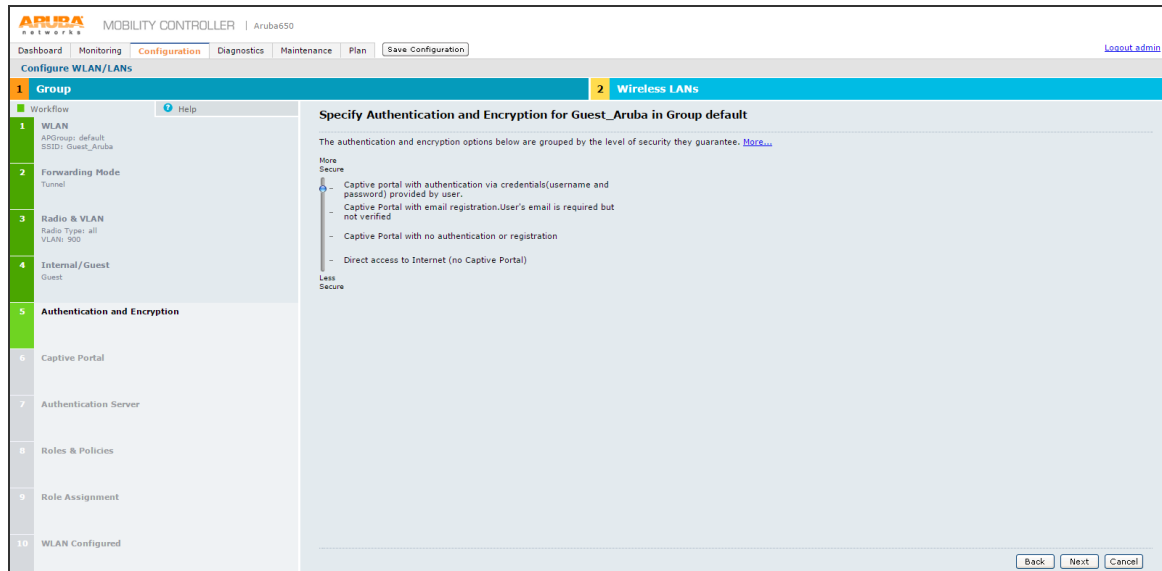


10. On Specify Radio Type and VLAN for Guest_Aruba in Group default screen select:
 - Radio Type - Select 'all' from the drop-down list.
 - VLAN - Select required options from the drop-down list and click the arrow button to include in the VLAN box.
11. Click **Next**.
12. The Specify whether WLAN is for Internal or Guest use for Guest_Aruba in Group default screen appears.

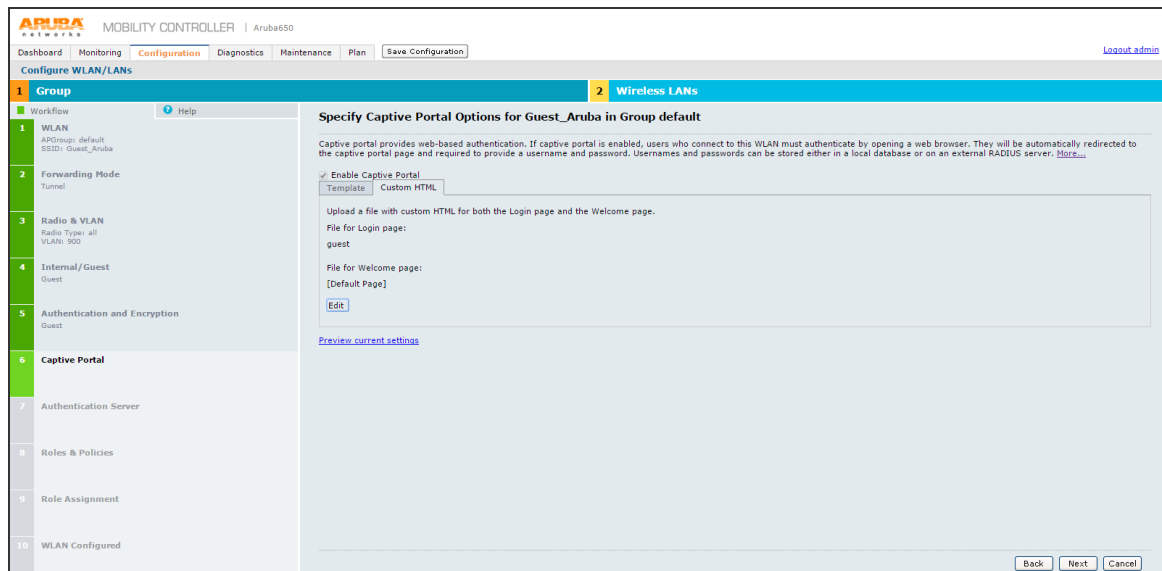


13. Specify whether WLAN is for Internal or Guest use for Guest_Aruba in Group default screen specify the purpose of the WLAN. Select Guest option for WLAN use and click **Next**.

14. The Specify Authentication and Encryption for Guest_Aruba in Group default screen appears.

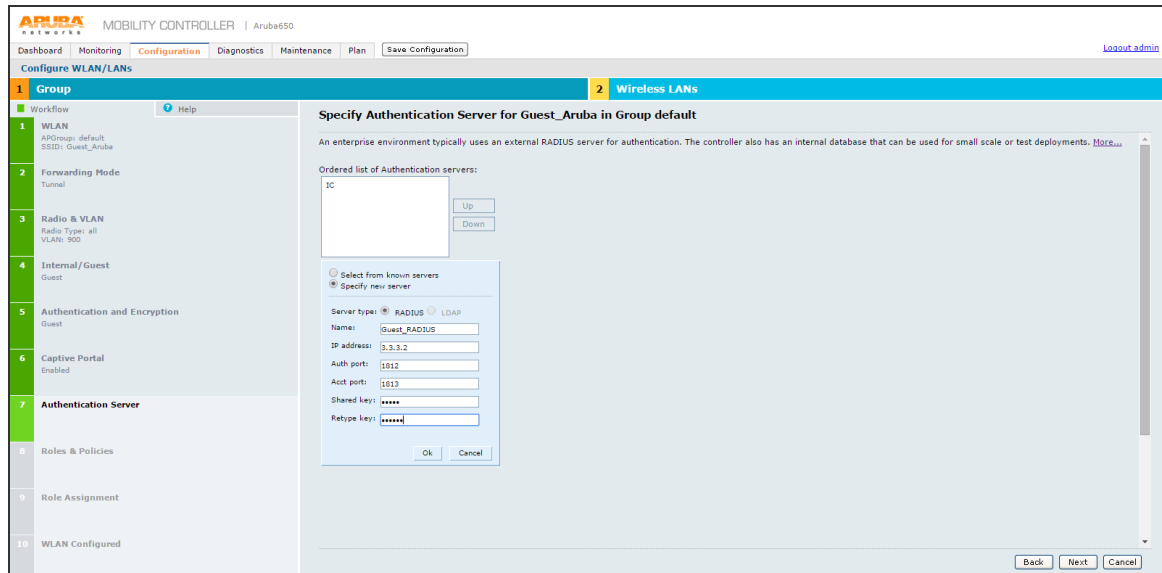


15. On Specify Authentication and Encryption for Guest_Aruba in Group default screen move the slider to Captive portal with authentication via credentials option and click Next. The Specify Captive Portal Options for Guest_Aruba in Group default screen appears.



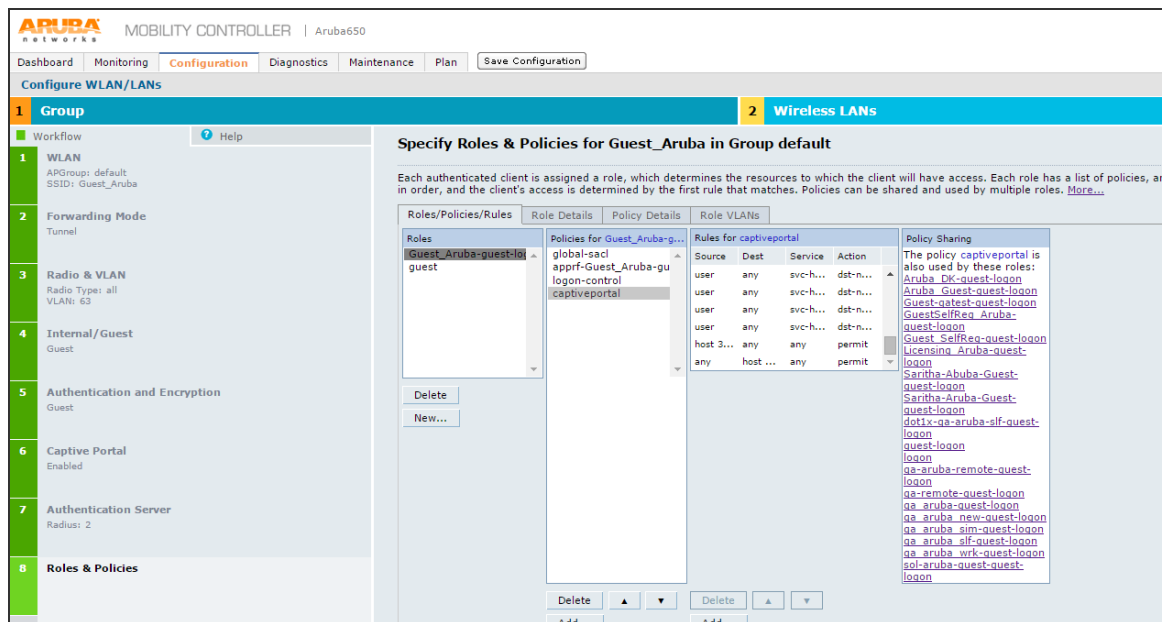
16. Specify Captive Portal Options for Guest_Aruba in Group default screen, click **Next**.

17. The Specify Authentication Server for Guest_Aruba in Group default screen appears.

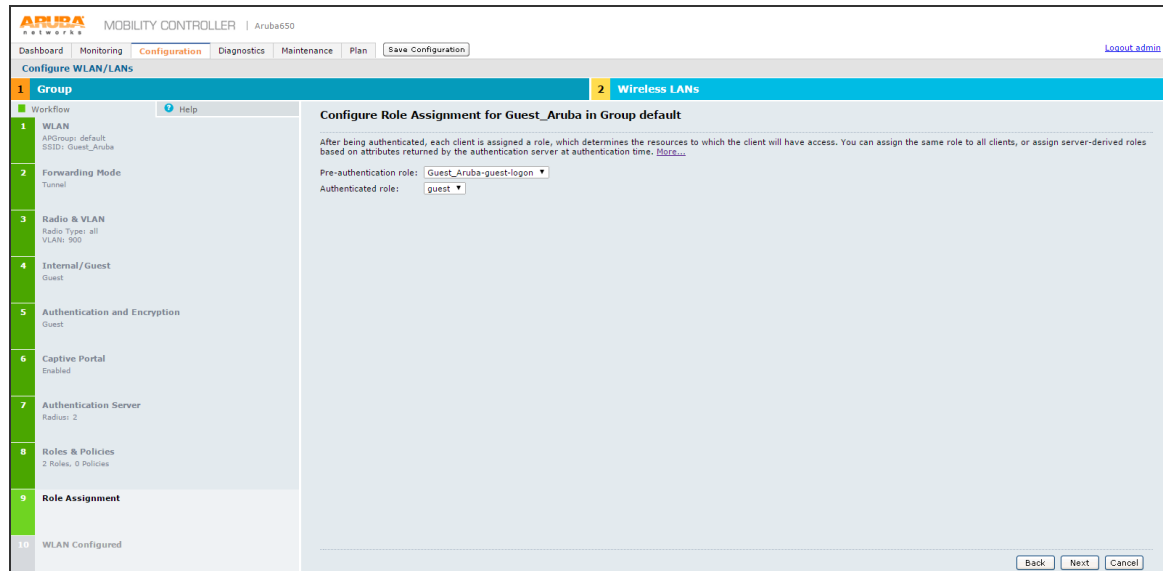


18. On Specify Authentication Server for Guest_Aruba in Group default screen, specify IPS server as the authentication server and click **Next**.

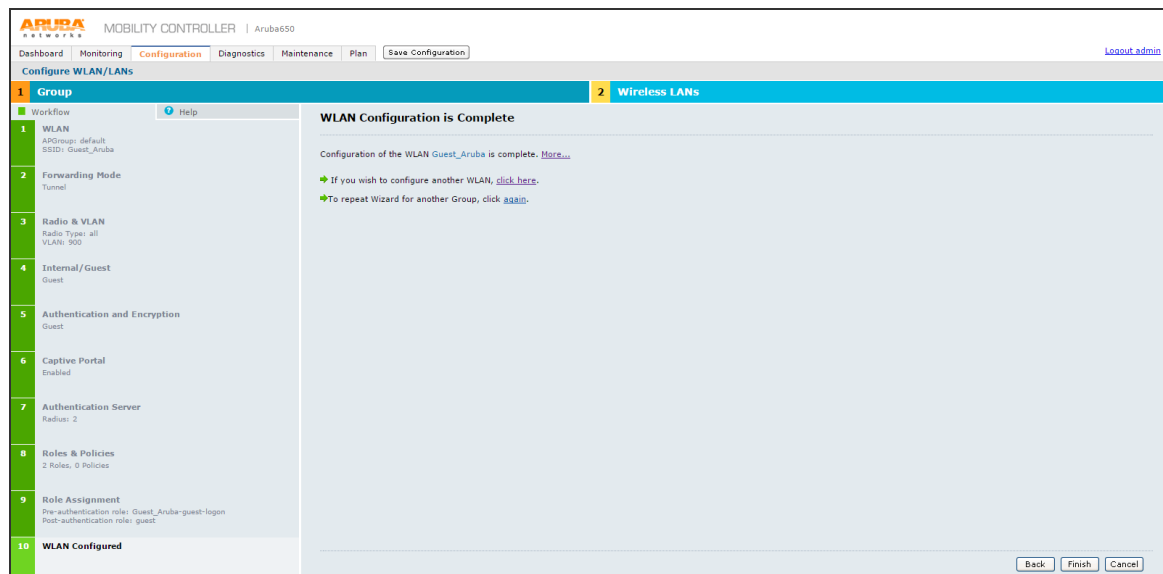
19. The Specify Roles & Policies for Guest_Aruba in Group default screen appears.



20. On Specify Roles & Policies for Guest_Aruba in Group default screen, configure the roles and click Next. The Configure Role Assignment for Guest_Aruba in Group default screen appears.

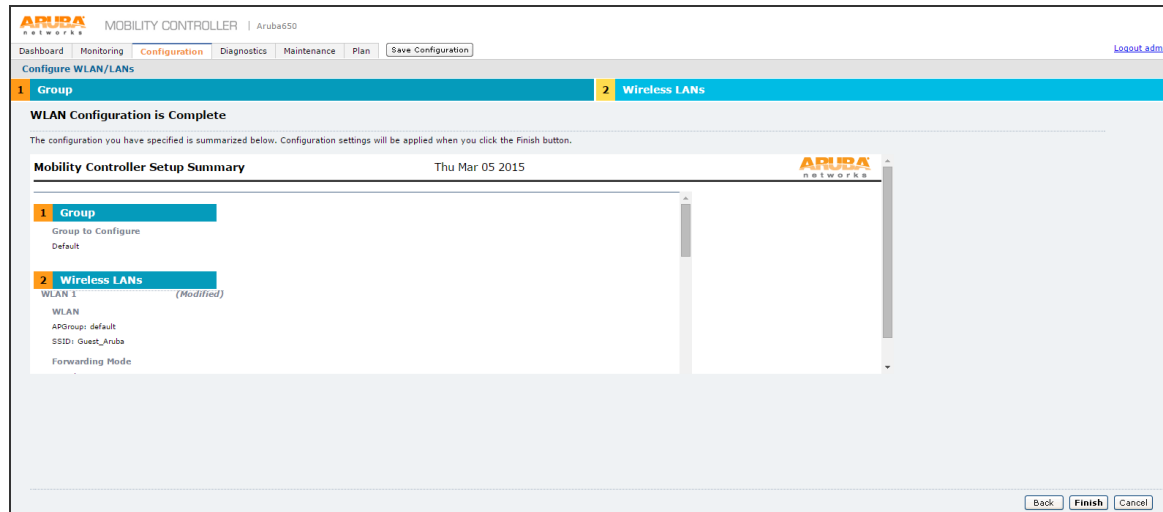


21. On Configure Role Assignment for Guest_Aruba in Group default screen, click **Next**.
22. The WLAN Configuration is Complete screen appears.

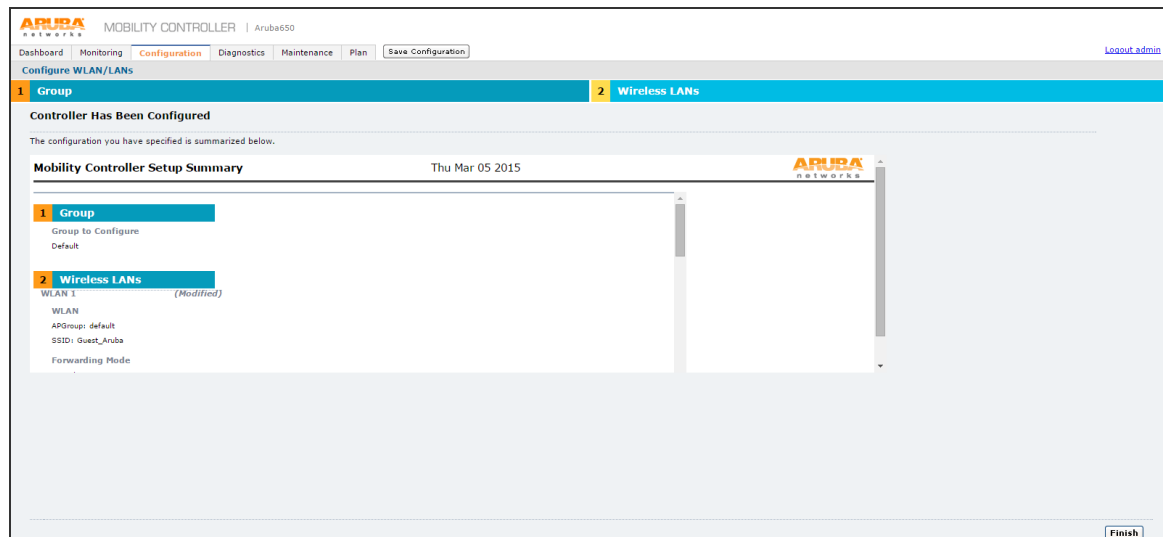


23. Click Finish to complete the configuration.

24. The WLAN Configuration is Complete screen appears displaying the summary of the configuration.

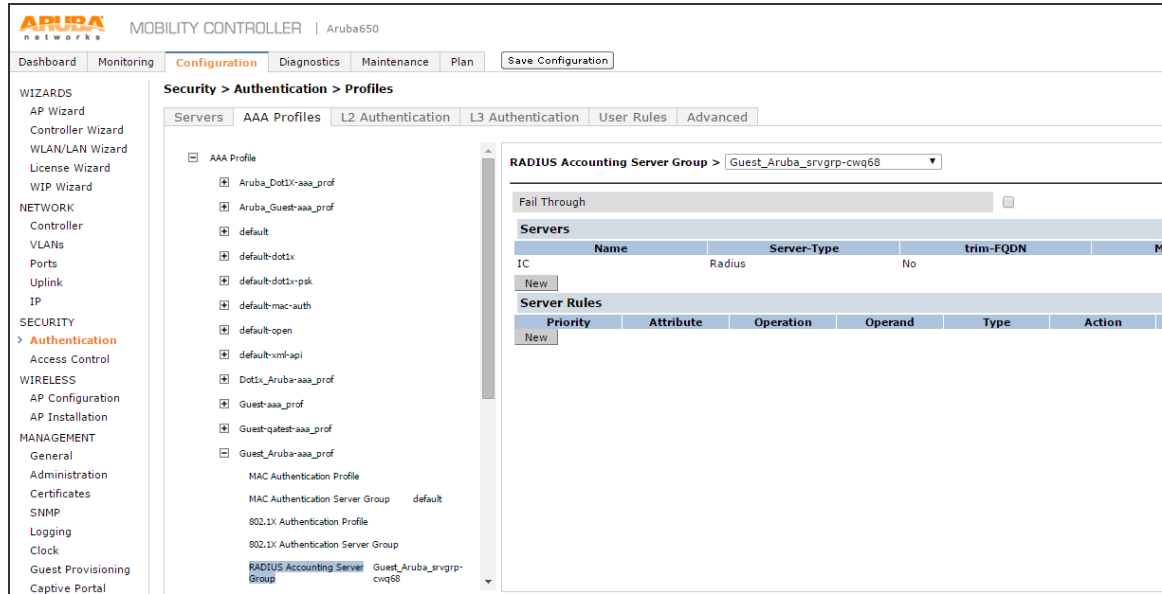


25. Click **Finish**.
26. The **Controller Has Been Configured** screen appears.



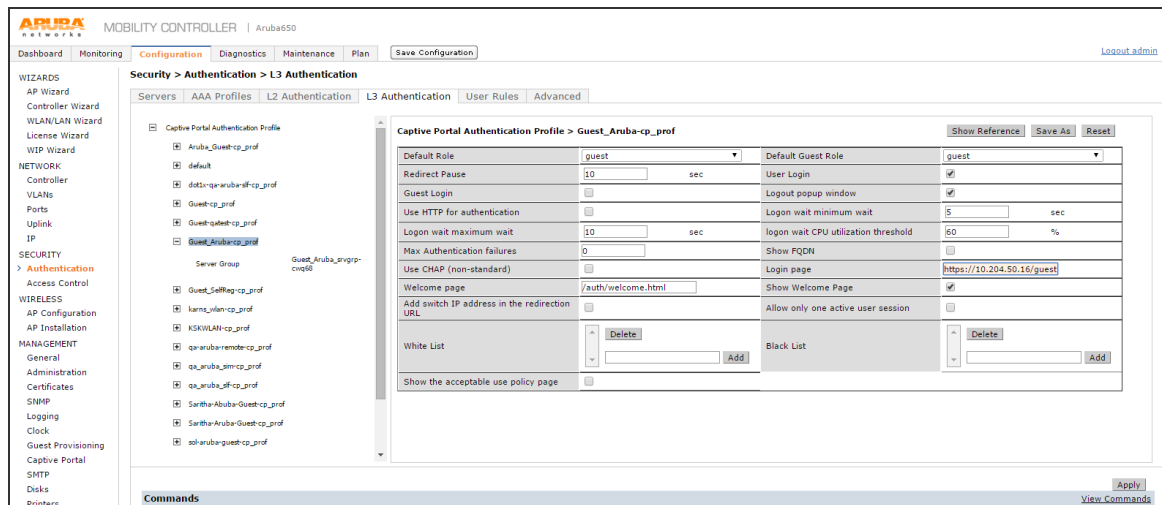
27. Click **Finish**.
28. The system refreshes and takes you to the Configuration tab.

29. Select **Security > Authentication > AAA Profiles** and click on **RADIUS Accounting Server Group**.
30. Select an appropriate server group for RADIUS Accounting Server Group.



External Captive Portal Configuration

1. In Aruba WLC select **Configuration > Security > Authentication > L3 authentication**.
2. The L3 authentication screen appears.



3. Click **Captive Portal Authentication Profile**. The list expands. Select the corresponding profile of the above configured WLAN.
4. Select the check box Add switch IP address in the redirection URL.
5. In the Login page box enter the IPS guest access URL that is configured as part of IPS configuration.
6. Click **Apply** to save the configuration.

RFC 3576 server configuration

1. In Aruba WLC go to **Configuration > Security > Authentication > Servers** tab. A list of configured servers is displayed.

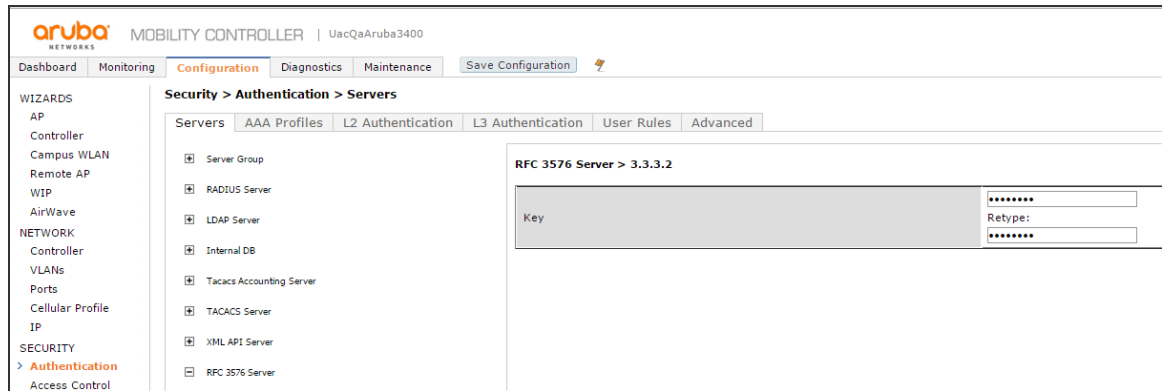
The screenshot shows the Aruba Mobility Controller configuration interface. The main content area displays the 'RFC 3576 Server' configuration page. The page includes a table of configured servers and an 'Add' button.

Instance	Actions
10.204.50.112	Show Reference Delete
10.204.50.16	Show Reference Delete
10.204.89.134	Show Reference Delete
10.204.89.166	Show Reference Delete
10.207.129.76	Show Reference Delete
10.209.113.211	Show Reference Delete

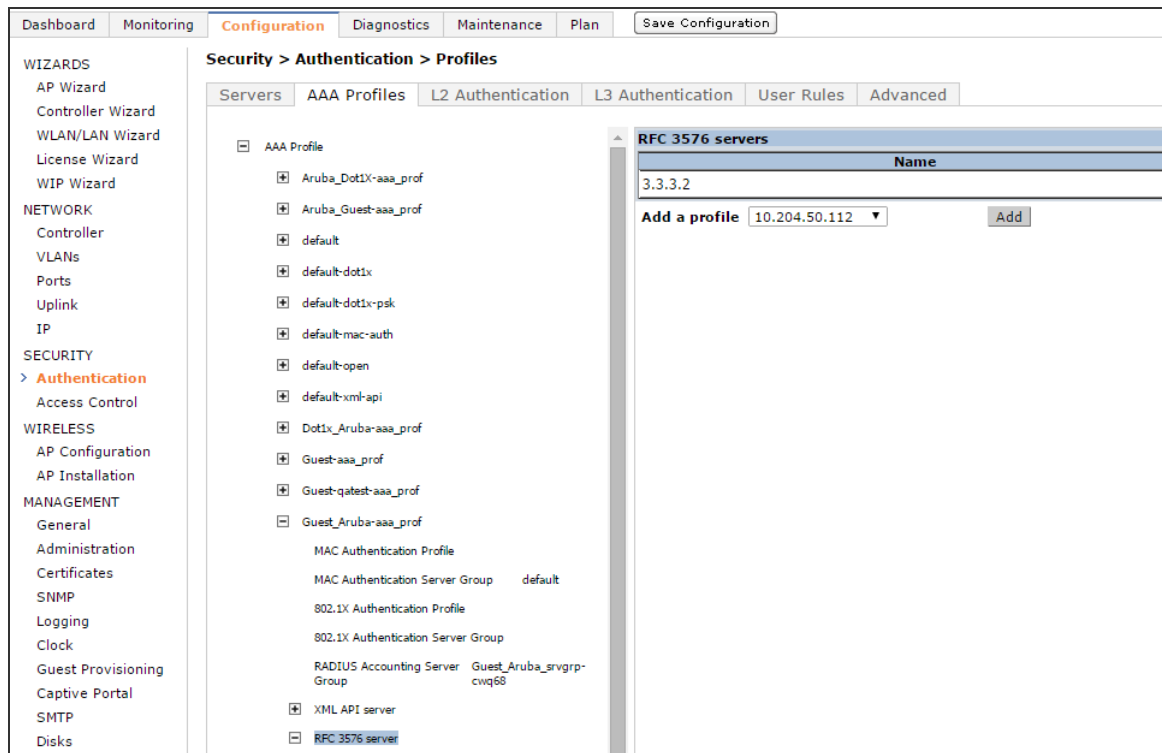
Below the table is an 'Add' button. The left sidebar shows the navigation menu with 'Authentication > Servers' selected.

2. Click the RFC 3576 Server and add IPS as RFC 3576 server, for supporting disconnect messages.

- Click on the RFC server that is newly created to provide the key.

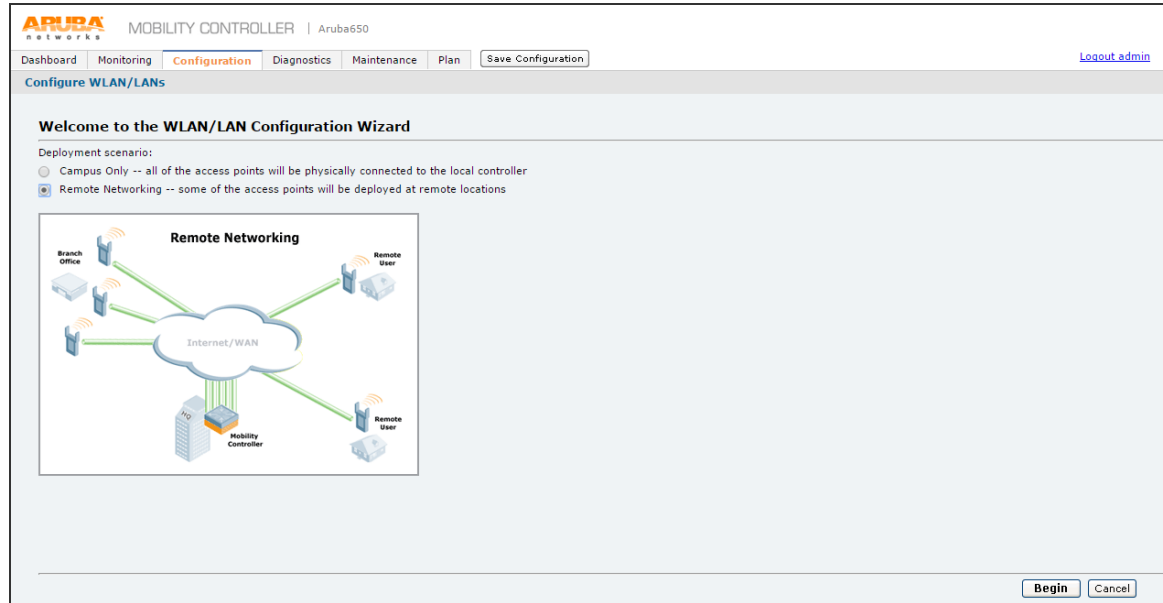


- Select **Security > Authentication > AAA Profiles**. Go to AAA profile and click on RFC 3576 server. Add the server that is newly created in step 1.

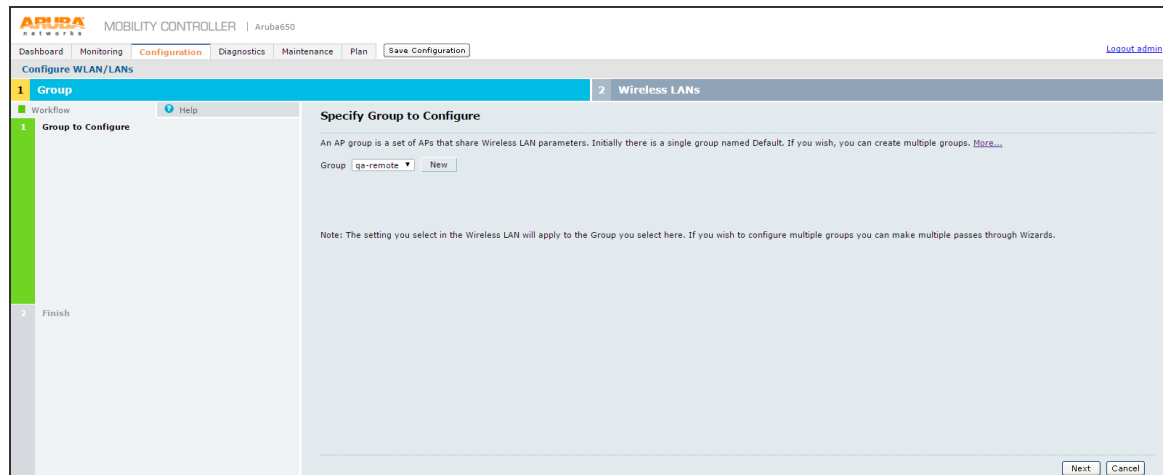


WLAN Configuration for Remote Networking mode on Aruba WLC

1. Log in to Aruba WLC. Select **Configuration > Wizards > WLAN/LAN Wizard**. The **Welcome to the WLAN/LAN Configuration Wizard** screen appears.



2. Select Remote Networking option and click **Begin**.
3. The **Specify Group to Configure** screen appears.



4. On the **Specify Group to Configure** screen, select an AP group and click **Next**.

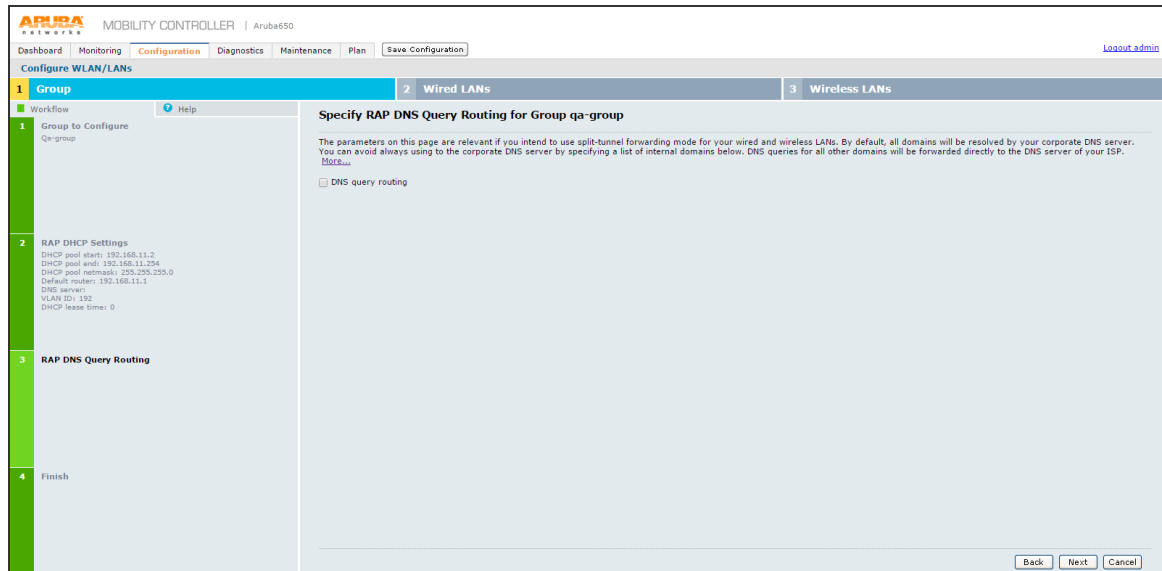
The screenshot shows the Aruba Mobility Controller configuration interface. The top navigation bar includes 'Dashboard', 'Monitoring', 'Configuration', 'Diagnostics', 'Maintenance', and 'Plan'. The 'Configuration' tab is active, and the 'Configure WLAN/LANs' section is selected. The main content area is titled 'Specify RAP DHCP Settings for Group qa-group'. A red arrow points to the 'Use internal DHCP server' checkbox, which is checked. Below this, there are input fields for DHCP pool start (192.168.11.2), DHCP pool end (192.168.11.254), DHCP pool netmask (255.255.255.0), Default router (192.168.11.1), DNS server, VLAN ID (192), and DHCP Lease time (Limit to: 30 Days, No Limit). The 'No Limit' radio button is selected. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

5. On the **Specify RAP DHCP settings for Group qa-group** screen, configure:

- DHCP pool start
- DHCP pool end
- DHCP pool netmask
- Default router
- DNS server
- VLAN ID
- DHCP Lease time – Select the required option and set the limit.

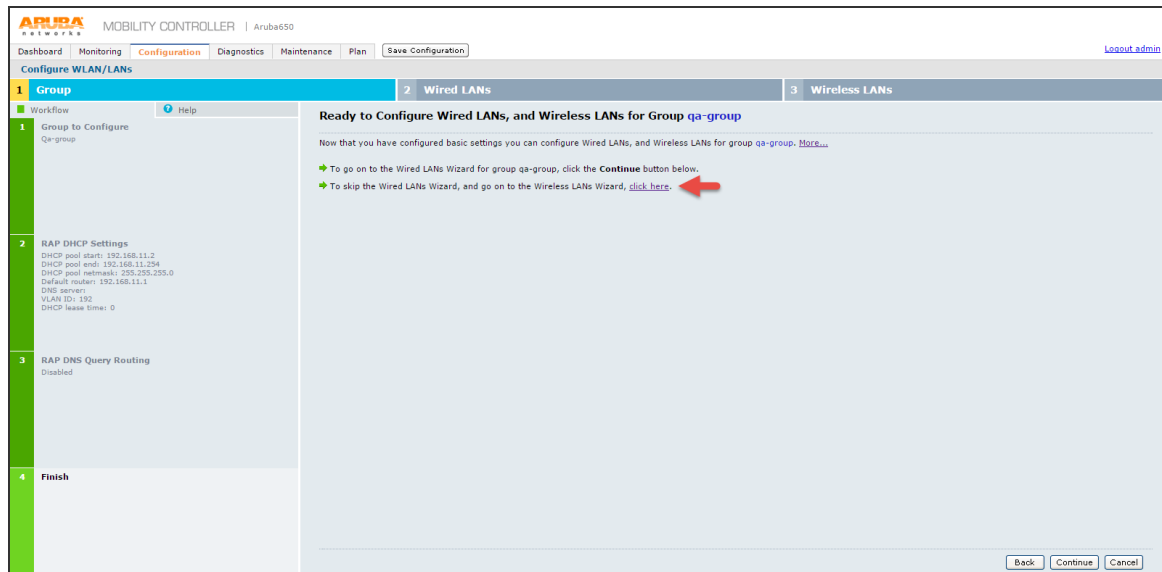
6. Click **Next**.

The **Specify RAP DNS Query Routing for Groups qa-group** screen appears.



7. On the **Specify RAP DNS Query Routing for Groups qa-group** screen click **Next**.

8. The **Ready to Configure Wired LANs, and Wireless LANs for Group** screen appears.



9. On the **Ready to Configure Wired LANs, and Wireless LANs for Group** screen, click the **Wireless LANs Wizard** link.
 - Follow the [Step 4](#) to [step 17](#) of Campus Only mode to complete Wireless WLAN configuration.
 - Follow [External Captive Portal Configuration](#) of Campus Only mode to configure Captive Portal for Remote Networking mode.
 - Follow [RFC 3576 server configuration](#) of Campus Only mode to configure IPS as RFC 3576 server.

Configuring Aruba WLC in campus only mode using CLI

To configure Aruba WLC for Guest Access in campus only mode via command-line interface, access the CLI in config mode and issue the following commands.

Configuring RADIUS server:

```
aaa authentication-server radius <RADIUS-profile-name>
host <IPS ip-address>
key <password>
```

Configuring Server Group:

```
aaa server-group <server-group-name>
auth-server <RADIUS-profile-name>
```

Configuring AAA profile:

```
aaa profile <AAA-profile-name>
```

Configuring SSID profile:

```
wlan ssid-profile <ssid-profile-name>
ssid <ssid-name>
ssid-enable
no hide-ssid
opmode opensystem
```

Configuring Captive portal:

```
aaa authentication captive-portal <CP-profile-name>
login-page <IPS-guest-URL>
switchip-in-redirectation-url
server-group <server-group-name>
user-logon
no guest_logon
default-role guest
```

Creating a User-role:

```
user-role <Role-Name>
captive-portal <CP-profile-name>
access-list session logon-control
access-list session captiveportal
```

Attaching initial-role to AAA profile:

```
aaa profile <AAA-profile-name>
initial-role <role-name>
```

Configuring Firewall policy rules for IPS: ip access-list session captiveportal

```
host <IPS-IP> any permit position 1
any host <IPS-IP> any permit position 2
```

Configuring Virtual-AP and associating SSID profile:

```
wlan virtual-ap <vap-profile-name>
forward-mode tunnel
vlan <vlan-id>
ssid-profile <ssid-profile-name>
aaa-profile <AAA-profile-name>
```

Configuring AP group and associating Virtual-AP profile:

```
ap-group default
# If it is another ap-group, give as required.
virtual-ap <vap-profile-name>
```

Configuring RFC-3576 server:

```
aaa rfc-3576-server <IPS-IP>
key <password>
```

Attaching RFC-3576 server to AAA profile:

```
aaa profile <aaa-profile-name>
rfc-3576-server <IPS-IP>
```

Attaching RADIUS accounting server group to AAA profile:

```
aaa profile <aaa-profile-name>
radius-accounting <server-group-name>
```

Configuring Aruba WLC in Remote Networking mode using CLI

To configure Aruba WLC for Guest Access in Remote Networking mode via command-line interface, access the CLI in config mode and issue the following commands.

Configuring RADIUS server:

```
aaa authentication-server radius <RADIUS-profile-name>
host <IPS ip-address>
key <password>
```

Configuring Server Group:

```
aaa server-group <server-group-name>
auth-server <RADIUS-profile-name>
```

Configuring AAA Profile:

```
aaa profile <AAA-profile-name>
```

Configuring SSID Profile:

```
wlan ssid-profile <ssid-profile-name>
ssid <ssid-name>
ssid-enable
no hide-ssid
opmode opensystem
```

Configuring Captive Portal:

```
aaa authentication captive-portal <CP-profile-name>
login-page <IPS-guest-URL>
switchip-in-redirectation-url
server-group <server-group-name>
user-logon
no guest_logon
default-role guest
```

Creating a User-role:

```
user-role <Role-Name>
captive-portal <CP-profile-name>
access-list session logon-control
access-list session captiveportal
```

Attaching initial-role to AAA profile:

```
aaa profile <AAA-profile-name>
initial-role <role-name>
```

Configuring Firewall policy rules for IPS:

```
ip access-list session captiveportal
host <IPS-IP> any any permit position 1
any host <IPS-IP> any permit position 2
```

Configuring Virtual-AP and associating SSID profile:

```
wlan virtual-ap <vap-profile-name>
forward-mode tunnel
vlan <vlan-id>
ssid-profile <ssid-profile-name>
aaa-profile <AAA-profile-name>
```

Configuring DHCP server on Remote AP:

```
ap system-profile <name>
rap-dhcp-default-router <ipaddr>
rap-dhcp-dns-server <ipaddr>
rap-dhcp-lease <days>
```

```
rap-dhcp-pool-start <ipaddr>
rap-dhcp-pool-end <ipaddr>
rap-dhcp-pool-netmask <netmask>
rap-dhcp-server-vlan <vlan>
```

Configuring AP group and associating Virtual-AP profile:

```
ap-group default
# If it is another ap-group, give as required.
virtual-ap <vap-profile-name>
    ap-system-profile <name>
```

Configuring RFC-3576 server:

```
aaa rfc-3576-server <IPS-IP>
key <password>
```

Attaching RFC-3576 server to AAA profile:

```
aaa profile <aaa-profile-name>
rfc-3576-server <IPS-IP>
```

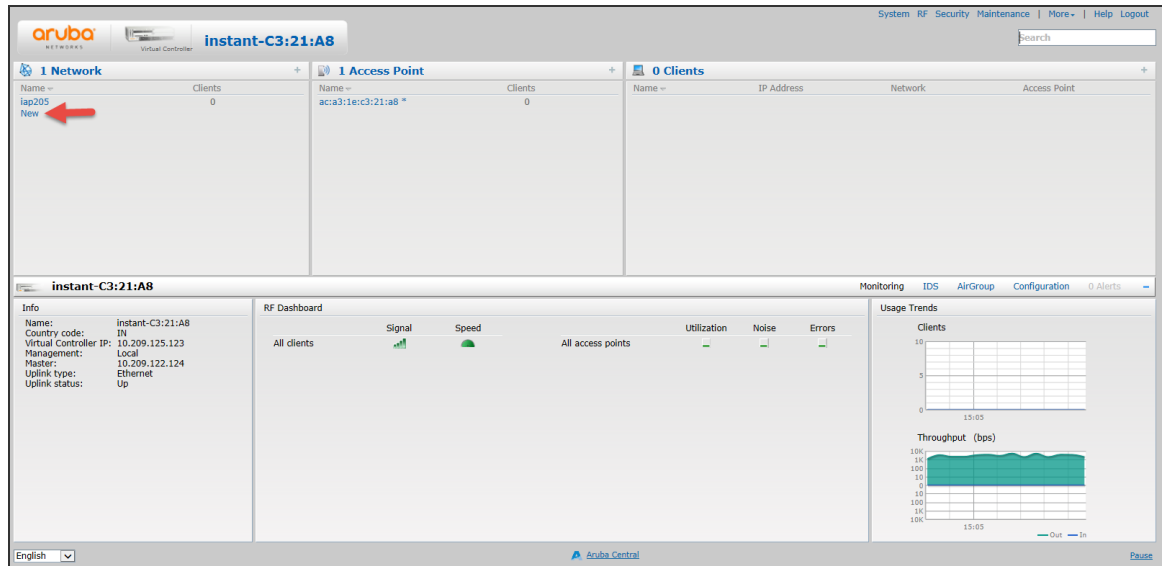
Attaching RADIUS accounting server group to AAA profile:

```
aaa profile <aaa-profile-name>
radius-accounting <server-group-name>
```

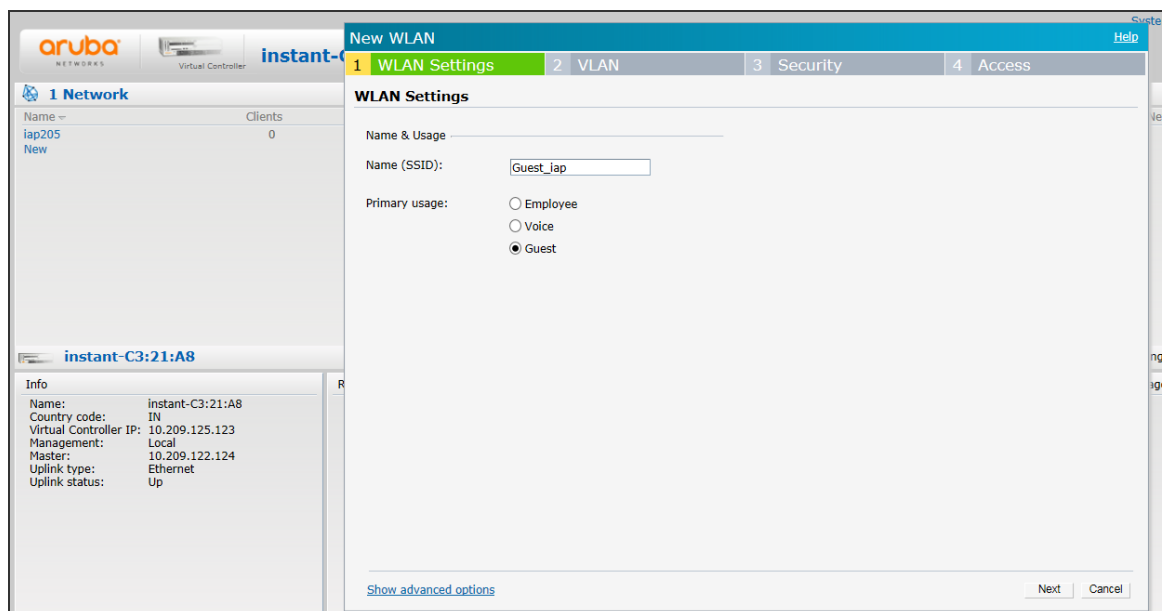
Configuring Aruba Instant Access Point

To configure Aruba Instant Access Point:

1. Login to the Aruba Instant Access portal. The Aruba Instant page appears.

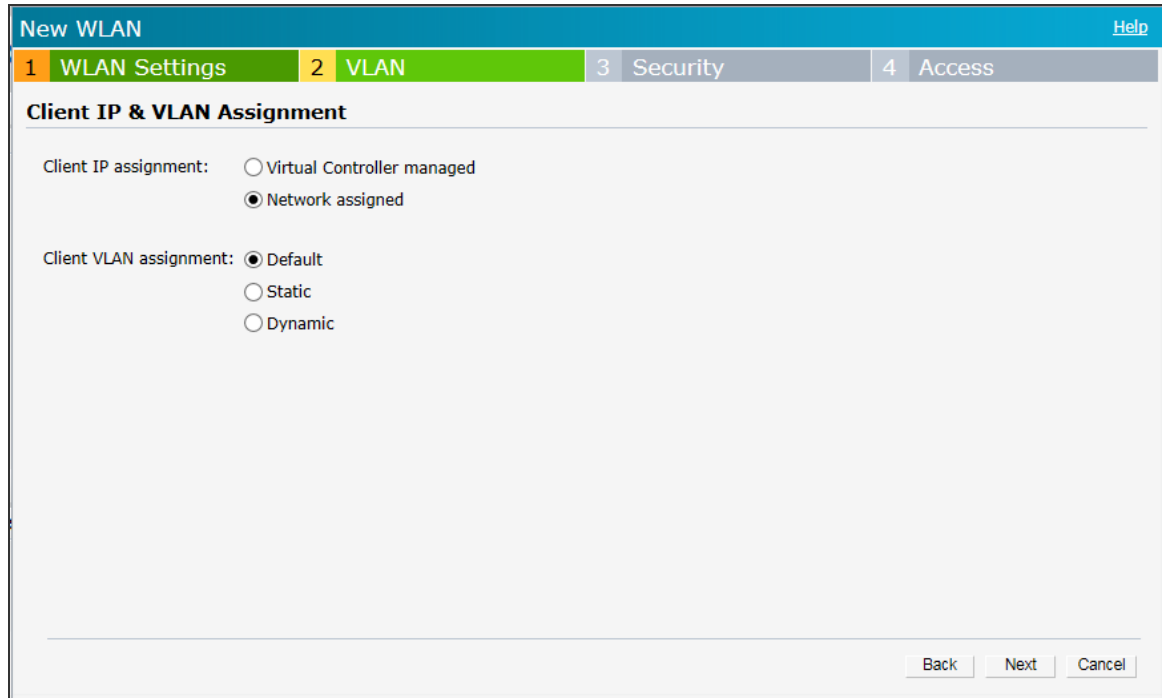


2. Click **New** to create a new SSID. The New WLAN window appears.



3. In the WLAN Settings tab:
4. In the New (SSID) field enter a name for the SSID.
5. In the Primary usage options select **Guest**.

6. Click **Next**.
7. The VLAN tab options appears.



The screenshot shows a web interface for configuring a new WLAN. The title is "New WLAN" with a "Help" link in the top right. Below the title is a navigation bar with four tabs: "1 WLAN Settings", "2 VLAN", "3 Security", and "4 Access". The "VLAN" tab is currently selected and highlighted in green. Below the navigation bar is the "Client IP & VLAN Assignment" section. It contains two groups of radio button options:

- Client IP assignment:
 - Virtual Controller managed
 - Network assigned
- Client VLAN assignment:
 - Default
 - Static
 - Dynamic

At the bottom right of the form, there are three buttons: "Back", "Next", and "Cancel".

8. Keep the DHCP setting as per your network design.
9. Client IP assignment here Network Assigned is chosen.
10. For Client VLAN assignment here **Default**. is chosen
11. Click **Next**.

12. The Security tab options appear.

The screenshot shows the 'New WLAN' configuration interface with the 'Security' tab selected. The 'Security Level' section is active, displaying a list of configuration options on the left and a detailed 'New' configuration window on the right. The 'New' window contains the following fields:

Field	Value
Splash page type	External
Captive portal profile	New
WISPr	New
MAC authentication Name	cap
Auth server 1 Type	Radius Authentication
Reauth interval IP or hostname	10.204.89.165
Internal server URL	/guest
Blacklisting Port	443
Walled garden Use https	Enabled
Disable if uplink type is Captive Portal failure	Deny internet
Encryption Automatic URL Whitelisting	Disabled
Redirect URL	(optional)

Buttons: Back, Next, Cancel, OK, Cancel

In the Security Level section do the following:

1. From the Security page type, drop-down list select External.
2. From the Captive portal profile, drop-down list select New
3. The **New** screen appears.
4. Enter the details as shown in the above figure and then click OK.

- The newly created captive portal appears in the Captive portal profile drop-down list.

The screenshot shows the 'New WLAN' configuration interface with the 'Security Level' tab selected. The 'Auth server 1' dropdown is set to 'New', which has opened a 'New Server' dialog box. The dialog shows 'RADIUS' selected, with fields for Name (ic), IP address (10.204.89.165), Auth port (1812), Accounting port (1813), Shared key, Retype key, Timeout (5 sec), Retry count (3), RFC 3576 (Enabled), Air Group CoA port (5999), NAS IP address, NAS identifier, Dead time (5 min), and various DRP fields.

- From the Auth server 1 drop-down list select New.
- The New Server screen appears.
- Create a server pointing to IPS server. Enter the details as shown in figure and then click OK.

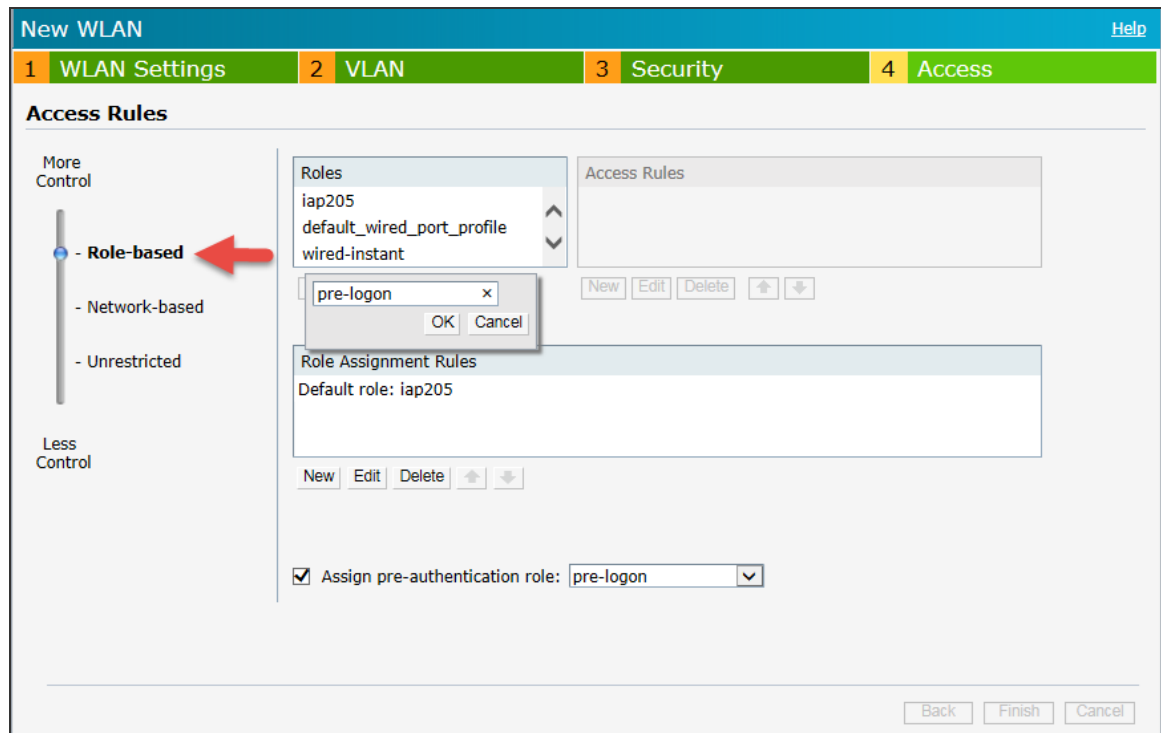
9. The configured Security tab options appear as in the following figure.

The screenshot shows the 'New WLAN' configuration interface with the 'Security' tab selected. The interface includes a breadcrumb trail: 1 WLAN Settings, 2 VLAN, 3 Security, and 4 Access. The 'Security Level' section contains the following settings:

- Splash page type: External
- Captive portal profile: cap
- WISPr: Disabled
- MAC authentication: Disabled
- Auth server 1: ic
- Auth server 2: -- Select Server --
- Reauth interval: 0 min.
- Accounting: Use authentication servers
- Accounting mode: Authentication
- Accounting interval: min.
- Blacklisting: Disabled
- Walled garden: [Blacklist: 0](#) [Whitelist: 0](#)
- Disable if uplink type is: 3G/4G Wifi Ethernet
- Encryption: Disabled

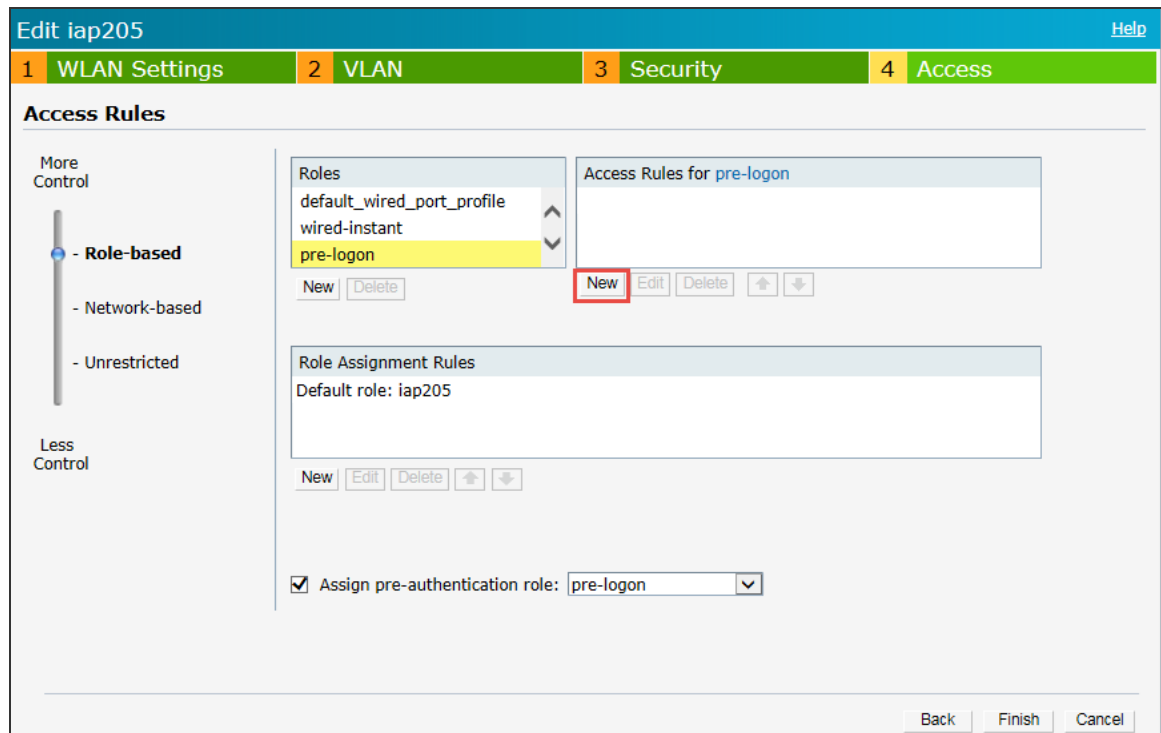
Navigation buttons at the bottom right are Back, Next, and Cancel.

- Click **Next**. The Access tab options appear.

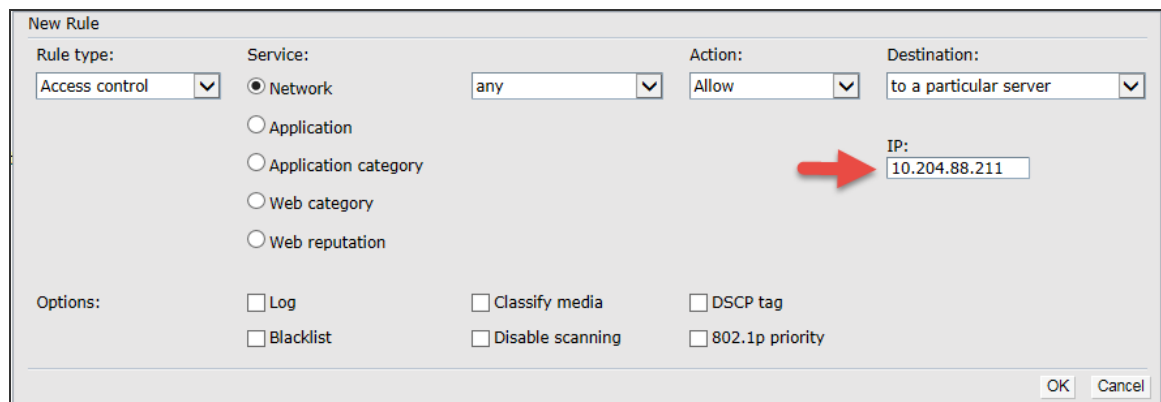


- In the Access Rules section:
- Move the slider to Role-based,

13. Under the Roles section, click New to create a new role 'pre-logout'.

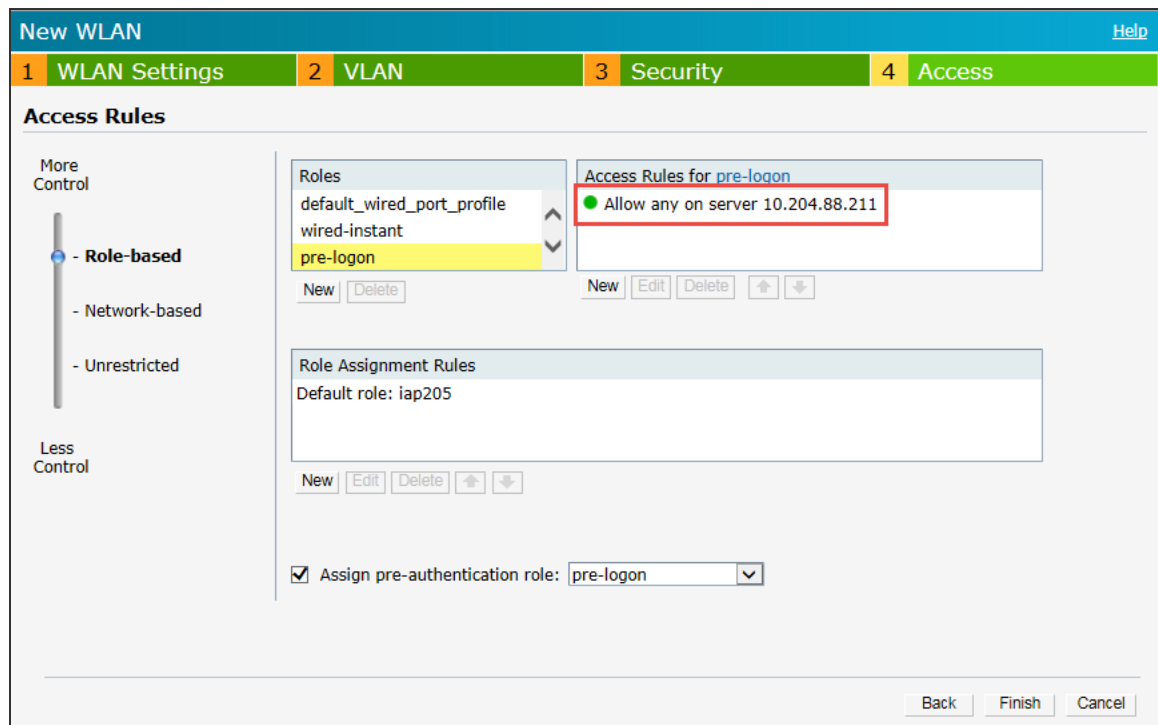


14. Under the Access Rules section click **New** to create an access rule for the role. The New Rule window appears.



15. Select the options as shown in the above figure.
16. From the Destination drop-down list select 'to a particular server'.
17. In the IP box enter the IPS server's IP address.

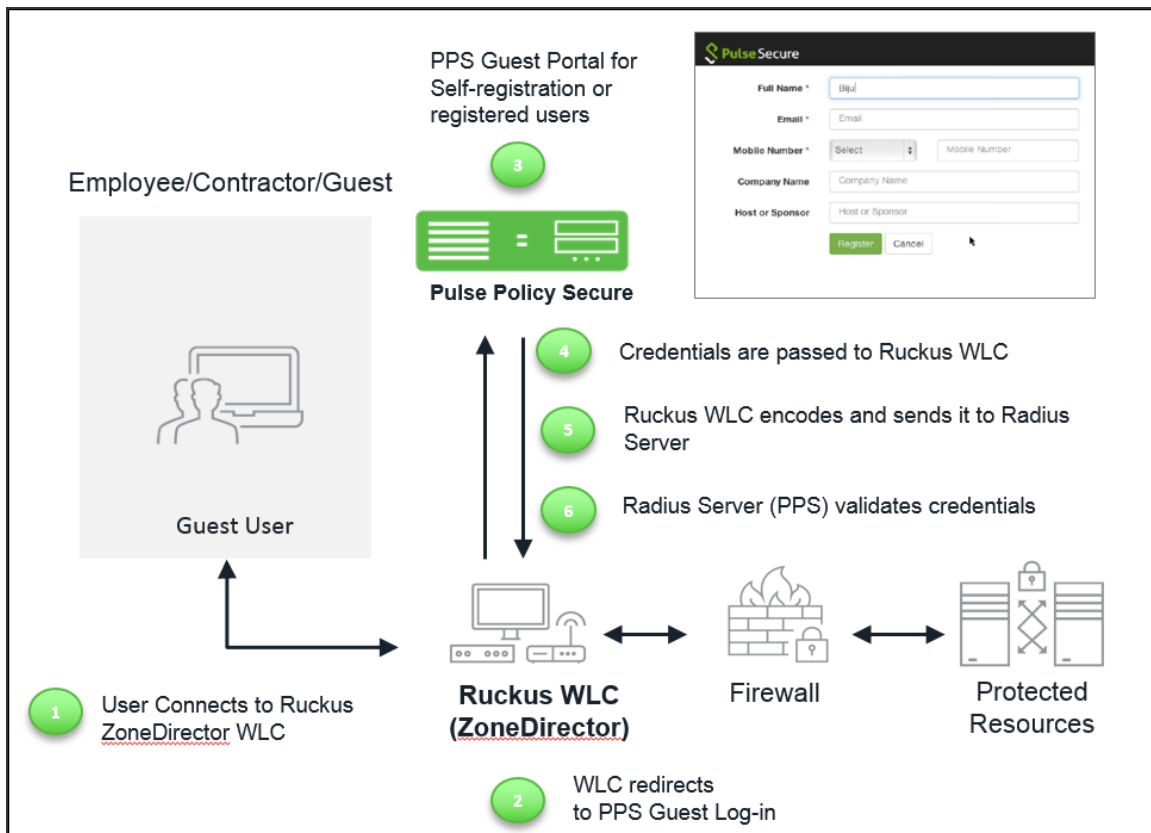
18. Click OK.
19. The Access Rule appears in the Access Rules for list box.



20. Select the Assign pre-authentication role check box and then select 'pre-logout' from the drop-down list.
21. Click **Finish** to complete the settings.

Configuring Ruckus WLC

Ruckus WLC is configured as Radius Client where IPS is the Radius Server. Figure illustrates the workflow of Guest Access on IPS for Ruckus WLC. This section provides examples of how to configure the Ruckus WLC. For more information, see *Ruckus documentation*.



To configure Ruckus WLC with IPS:

1. Connect user/endpoint to the Ruckus Wireless network with open SSID over 802.1X with restricted access through ACLs.
2. Redirect Ruckus WLC guest to external (IPS) captive portal when guest tries to access a web-resource.
3. Enter credentials on captive portal page.
4. For guest access authentication, IPS provides guest user credentials to Ruckus SmartZone WLC's management interface via REST API.
5. Ruckus WLC can encode the credentials and send it to a RADIUS server (IPS) through Radius Access Request.
6. The RADIUS server validates the credentials and sends a RADIUS response, which contains standard RADIUS attributes and Vendor Specific Attributes.

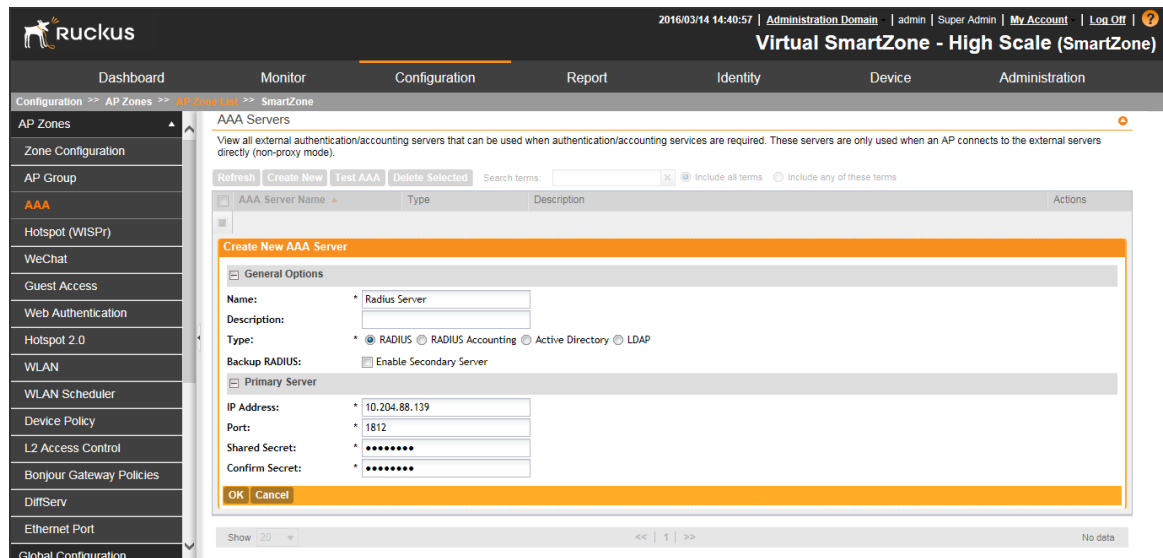
7. Ruckus WLC provides network access to the guest by changing VLAN based on IPS role-based policy.

Ruckus SmartZone WLC Configuration

The Ruckus SmartZone software platform provides unified software architecture across wireless LAN (WLAN) controllers, for appliance, virtualized and cloud environments for deployment flexibility.

To configure SmartZone WLC:

1. Configure IPS as Radius Sever.
2. Select **Configuration > AP Zone > Zone Name > AAA servers> Create New**.
3. Configure Name, IP Address, Shared Secret and Confirm Secret.



To configure Hotspot (WISPr) service:

1. Select **Configuration > AP Zone > Zone Name > Hotspot (WISPr) > Create New**.

The screenshot shows the Ruckus Virtual SmartZone - High Scale (SmartZone) configuration interface. The left sidebar contains a navigation menu with options like Zone Configuration, AP Group, AAA, Hotspot (WISPr), WeChat, Guest Access, Web Authentication, Hotspot 2.0, WLAN, WLAN Scheduler, Device Policy, L2 Access Control, Bonjour Gateway Policies, DiffServ, Ethernet Port, Global Configuration, and AP Tunnel Profiles. The main content area is titled 'Create New Hotspot Portal' and includes the following fields and options:

- General Options:** Portal Name (HotSpot), Portal Description.
- Redirection:** Smart Client Support (None, Enable, Only Smart Client Allowed), Logon URL (Internal, External), Redirect unauthenticated user to the URL for authentication (https://10.204.88.139/guest), Redirected MAC Format (AA:BB:CC:DD:EE:FF), Start Page (Redirect to the URL that user intends to visit, Redirect to the following URL).
- User Session:** Location Information, Walled Garden.

Buttons for 'OK' and 'Cancel' are visible at the bottom of the form.

2. Configure Portal Name, Login URL text box with https://IPS-ip/guest.
3. Configure Northbound Interface password as Ruckus Request Password on Radius Client page in IPS.

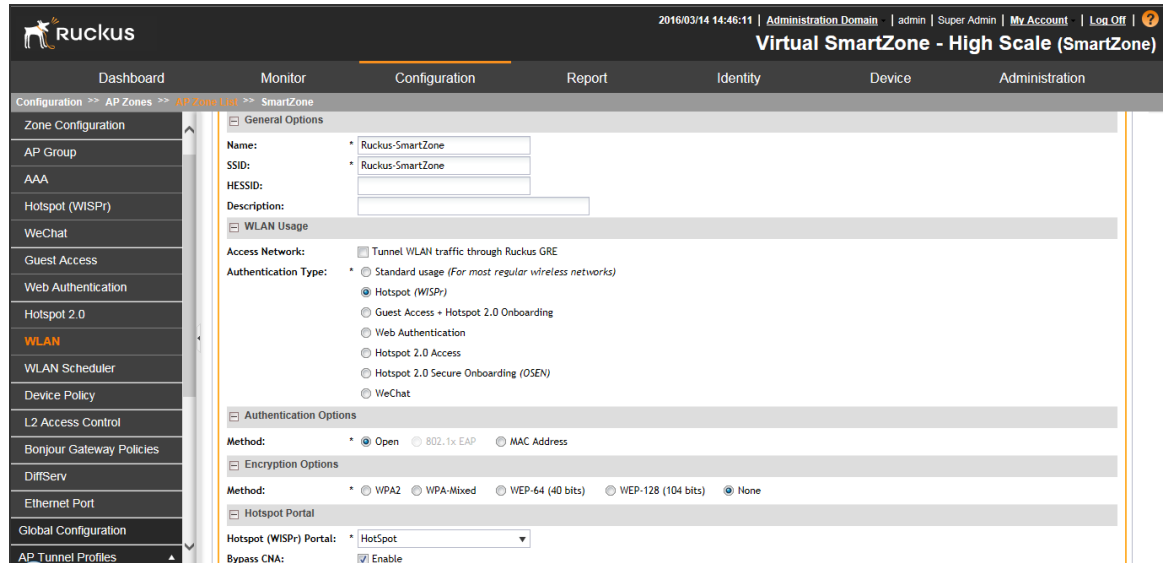
The screenshot shows the Ruckus Virtual SmartZone - High Scale (SmartZone) configuration interface. The left sidebar contains a navigation menu with options like General System Settings, System Time, Syslog Server, Northbound Portal Interface, SMTP Server, FTP Server for Uploading Statistical Data, Critical AP Rules, Manage User Agent Blacklist, Node Affinity, Certificate Store, Cluster & Planes, Cluster Planes, Cluster Redundancy, Network Management, SNMP Agent, and Event Management. The main content area is titled 'Northbound Portal Interface' and includes the following fields and options:

- Northbound Portal Interface:** Set the northbound portal interface password. 3rd party applications use the northbound portal interface to authenticate users and to retrieve user information during the UE association. Password field (masked with dots).

Buttons for 'Refresh', 'Apply', and 'Cancel' are visible below the password field.

To configure WLAN:

1. Select **Configuration > AP Zone > Zone Name > WLAN > Create New**.
2. Configure Name, SSID, Authentication type as "Hotspot (WIPSr) ", Authentication Method as "open" and Encryption as "None".
3. Select Hotspot configured from drop down list and select Authentication Server.

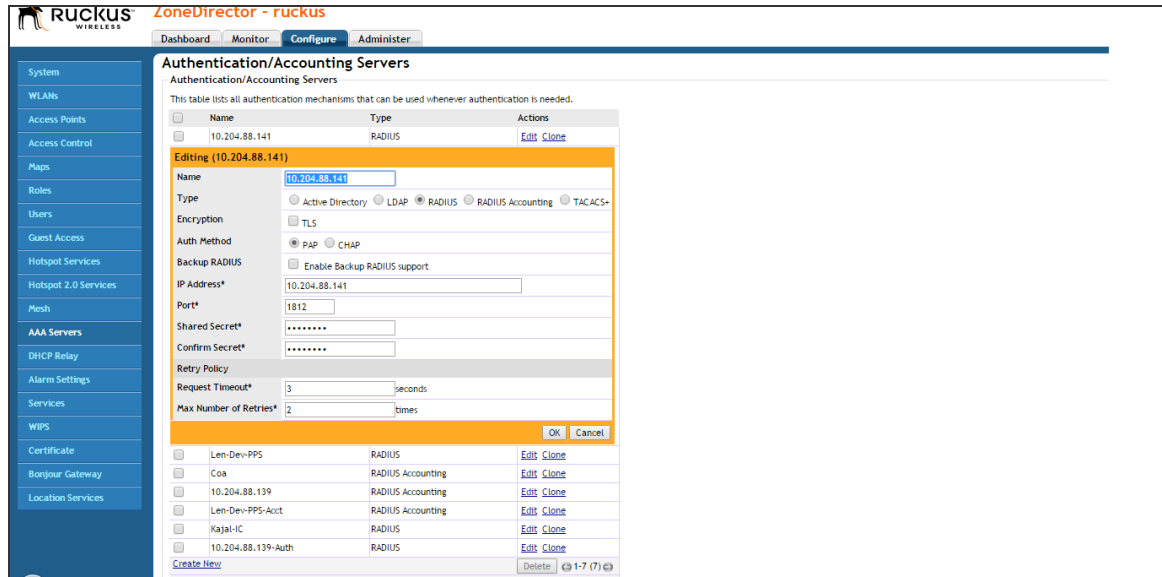


Ruckus ZoneDirector WLC Configuration

The following steps give configuration of Ruckus ZoneDirector WLC:

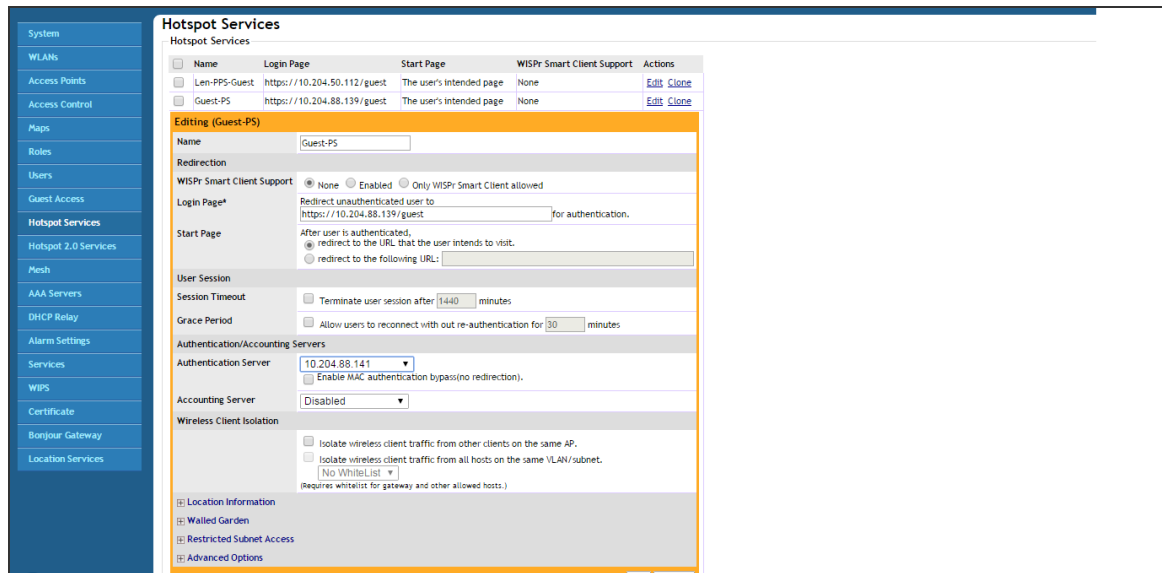
1. Configure IPS as Radius Sever.
2. Select **Configuration > AP Zone > Zone Name > AAA servers > Create New**.

3. Enter Name, select "Type" as "Radius", IP Address, Shared Secret and Confirm Secret.



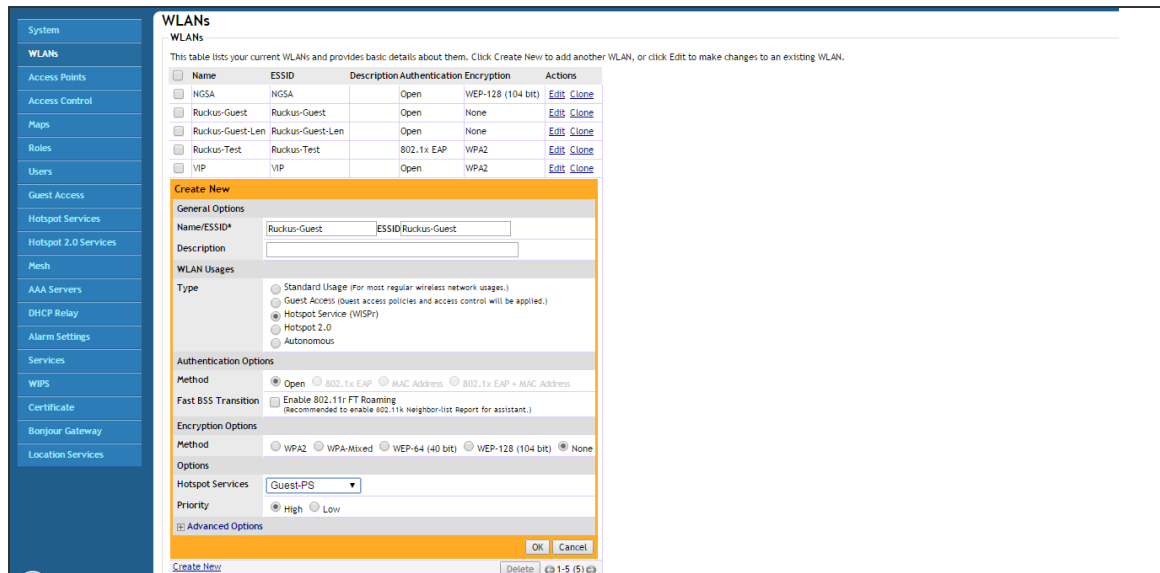
To configure Hotspot (WISPr) service:

1. Select **Configuration > AP Zone > Zone Name > Hotspot Services>Create New.**
2. Configure Name, Login page text box with https://IPS-ip/guest.
3. Select authentication server configured in AAA servers.



To configure WLAN:

1. Go to **Configuration > AP Zone > Zone Name > WLAN > Create New**.
2. Enter the Name, SSID, Authentication type as "Hotspot (WIPSR)", Authentication method as "Open" and Encryption as "None".
3. Select Hotspot services as "Guest PS" from drop down list.



4. Click **OK** to save changes to the settings.

Verifying Device Certificates

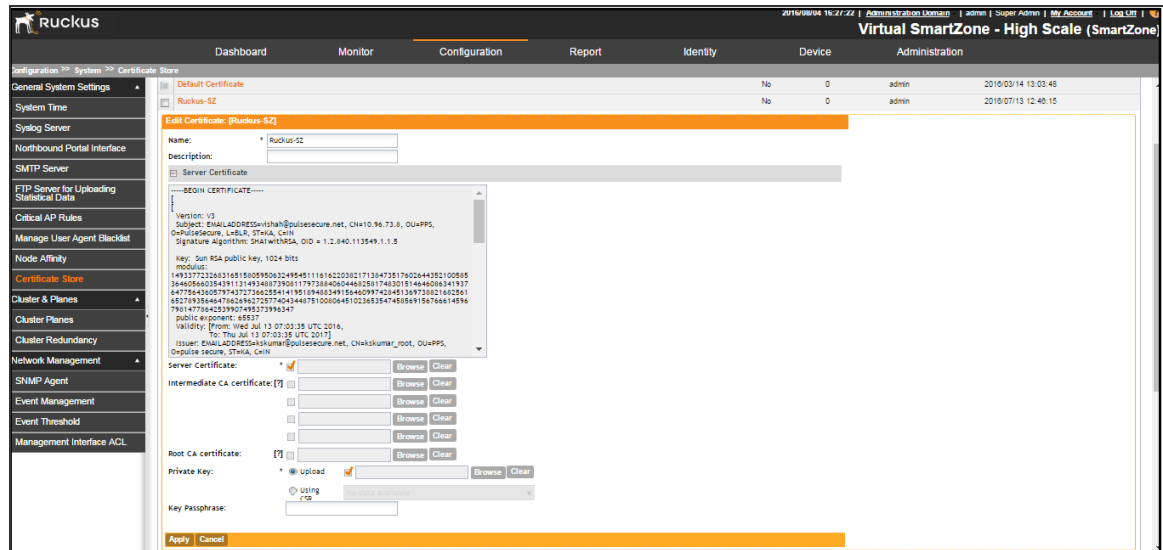
Ruckus device certificate validation enhances the security between IPS and the Ruckus device for guest access. It allows IPS to verify whether the server certificate is from a trusted source. This topic describes how to configure the IPS for validating device certificates, create certificates on Ruckus, and check the validity of the certificate.

Step1: Creating a Server Certificate

To create a CSR:

1. From Certificate Server generate a Server Certificate with private key and import the certificate on Ruckus SmartZone.

- To import the certificate on Ruckus, select **Configuration > System > Certificate Store > Import**.



Step2: Importing the Certificate on IPS

To import the certificate on IPS:

- Obtain the root CA from the certificate server for the generated certificate.
- Select **System > Configuration > Certificates > Trusted Server CAs > Import Trusted Server CA** and import the certificate.

Step3: Adding Ruckus Wireless device as RADIUS Client

To add Ruckus wireless device to IPS:

- Select **Endpoint policy > Network Access > RADIUS Client > New RADIUS Client**.
- Select Ruckus Wireless as a Radius client and enable Ruckus Server Certificate Validation.
- (Optional) From client machine, perform a guest authentication, if the guest user is able to authenticate then the certificate is valid. Otherwise it is an invalid certificate or certificate is not available.
- (Optional) Verify the event logs to check if there are any certificate invalid logs.

Cisco Meraki WLC Configuration

The following steps give configuration of Cisco Meraki WLC:

1. Configure IPS as Radius Sever.
2. Select **Wireless > Access Control > Select SSID.**

3. Configure Radius Authentication and Accounting Server for the Splash page.

Meraki

Search Dashboard

Announcements Help

Access control

SSID: meraki_wlc

Network access

Association requirements

- Open (no encryption)
Any user can associate
- Pre-shared key with WPA2
Users must enter a passphrase to associate
- MAC-based access control (no encryption)
RADIUS server is queried at association time
- WPA2-Enterprise with Meraki authentication
User credentials are validated with 802.1X at association time

Splash page

- None (direct access)
Users can access the network as soon as they associate
- Click-through
Users must view and acknowledge your splash page before being allowed on the network
- Sponsored guest login
Guests must enter a valid sponsor email and own email address before being allowed on the network
- Sign-on with my RADIUS server
Users must enter a username and password before being allowed on the network
- Sign-on with SMS Authentication
Users enter a mobile phone number and receive an authorization code via SMS. After a trial period of 25 texts, you will need to connect with your Twilio account on the [Network-wide settings](#) page.
- Cisco Identity Services Engine (ISE) Authentication
Users are redirected to the Cisco ISE web portal for device posturing and guest access
- Systems Manager Sentry enrollment
Only devices with Systems Manager can access this network
- Billing (paid access)
Users choose from various pay-for-access options, or an optional free tier

RADIUS for splash page

#	Host	Port	Secret	Status	Actions
1		1812	OK	✚ ✕ Test

[Add a server](#)

RADIUS accounting

RADIUS accounting is enabled

RADIUS accounting servers

#	Host	Port	Secret	Status	Actions
1	..3	1813		✚ ✕

[Add a server](#)

Enable data-carrier detect? DCD is enabled

IP addresses

The Meraki cloud must be able to communicate with your RADIUS servers via the Internet.

Please make sure that:

- Your RADIUS servers have public IP addresses (i.e., they are reachable on the Internet).
- Your firewall, if any, allows incoming traffic to your RADIUS servers.
- You whitelist IP addresses as clients on your RADIUS server as per the [firewall information page](#).

Failover policy

If none of your RADIUS servers are reachable, should clients be allowed to use the network?

- Deny access
- Allow access

Load balancing policy

- Strict priority order
- Round robin

Network access control

Disabled: do not check clients for antivirus software

Assign group policies by device type

Disabled: do not assign group policies automatically

Captive portal strength

Block all access until sign-on is complete

Walled garden

Walled garden is enabled

Walled garden ranges

4. Navigate to **Wireless > Splash Page**. Configure the IPS URL where the users will be redirected.

The screenshot displays the Cisco Meraki dashboard interface for configuring a splash page. The left sidebar shows the navigation menu with 'Wireless' selected. The main content area is titled 'Splash page' and shows the SSID 'meraki_wlc'. A red box highlights the 'Custom splash URL' section, which includes a radio button for 'Or provide a URL where users will be redirected:' and a text input field containing 'https://.../3/guest'. Below this, there are sections for 'Customize your page' (Message), 'Customize your consent message' (Network user consent: Off), 'Splash logo' (No logo), 'Splash language' (English), and 'Splash behavior' (Splash frequency: Every half hour, Where should users go after the splash page?: The URL they were trying to fetch). At the bottom, there are buttons for 'Save changes', 'Preview', and 'cancel', along with a 'Make a wish' button. The footer contains copyright information and session details.

For more information, see Meraki documentation.

Example Configuration: Guest Access with Huawei WLC/Switch

The goal is to provide secure and role-based access control for Guest Access using ACLs on Huawei WLC/Switch through Ivanti Policy Secure.

Configuring Ivanti Policy Secure

1. Use the Default Guest Authentication Server under **Authentication > Auth.Servers**.

Authentication Servers

Enable Auth Traffic Control

New: (Select server type)

10 records per page Search:

<input type="checkbox"/>	Authentication/Authorization Servers	Type
<input type="checkbox"/>	Administrators	Local Authentication
<input type="checkbox"/>	Certificate Authentication	Certificate Server
<input type="checkbox"/>	Guest Authentication	Local Authentication
<input type="checkbox"/>	Guest Wired Authentication	MAC Address Authentication

The Guest configuration page is shown below.

Auth Servers > Guest Authentication > Settings

Settings

Settings | Users | Admin Users

*Name: Label to reference this server.

▼ Password Options

Minimum length: characters

Maximum length: characters

Password must have at least digits

Password must have at least letters

Password must have mix of UPPERCASE and lowercase letters

Password must be different from username

New passwords must be different from previous password

Password stored as clear text This option can only be set during create
Note: If password stored as clear text, more authentication protocols, i.e. CHAP, EAP-MD5, are supported

▼ Password Management

Allow users to change their passwords

Force password change after days

Prompt users to change their password days before current password expires

Note: Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities

▼ Account Lockout

Enable Account Lockout for users

Maximum wrong password attempts: (3 and above)

Account Lockout period (minutes): (10 and above)

▼ Guest Access

Guest User Account Managers

Enable Guest User Account Managers to administer Guest Accounts Configure system [GUAM settings](#)

Instructions for Guest User Account Manager:
Instructions displayed for guest users creation and updation. You can use ,
, , <noscript>, and <a href> tags to format the text.

Maximum Account Validity Period: Set the Guest Account length limit (end time minus start time) in hours. This is valid for guests created by Guest Admin. Does not impact existing user expiration.

Guest Self-Registration

Send guest user credentials via: SMS Email Configure [SMS/Email settings](#)

Show credentials on screen after guest completes registration

Enable Sponsored Guest Access

Maximum Account Validity Period for Self Registered Guests: Set the Guest Account length limit in hours. This is valid for self registered guests. Does not impact existing user expirations.

Note: To enable Guest Self-Registration navigate to Signing In > Sign-in Policies > User URLs > [url] > [Configure Guest Settings](#)

Common configuration for Guest User Account Managers and Guest Self-Registration

Guest User Name Prefix: Prefix applied to auto-generated user names.

Guest User Info Fields: Enter additional fields for guest user information, one field per line. For example:
Title
Company name
Sponsor

2. Select **User Realms > User Authentication Realms**.

User Realms > User Authentication Realms

User Authentication Realms

View: Overview for all realms Update

New... Duplicate... Delete...

10 records per page Search:

Authentication Realm	Servers	Dynamic Policy Evaluation
<input type="checkbox"/> Cert Auth	Primary: Certificate Authentication	Disabled
<input type="checkbox"/> Guest	Primary: Guest Authentication	Disabled
<input type="checkbox"/> Guest Admin	Primary: Guest Authentication	Disabled
<input type="checkbox"/> Guest Sponsor	Primary: Guest Authentication	Disabled
<input type="checkbox"/> Users	Primary: System Local Device, MDM, MobileIron	Disabled

3. Select **Authentication > Signing In > Sign-in Policies**.

Signing In > Sign-In Policies

Sign-in Policies Sign-In Pages Sign-In Notifications Authentication Protocol Sets

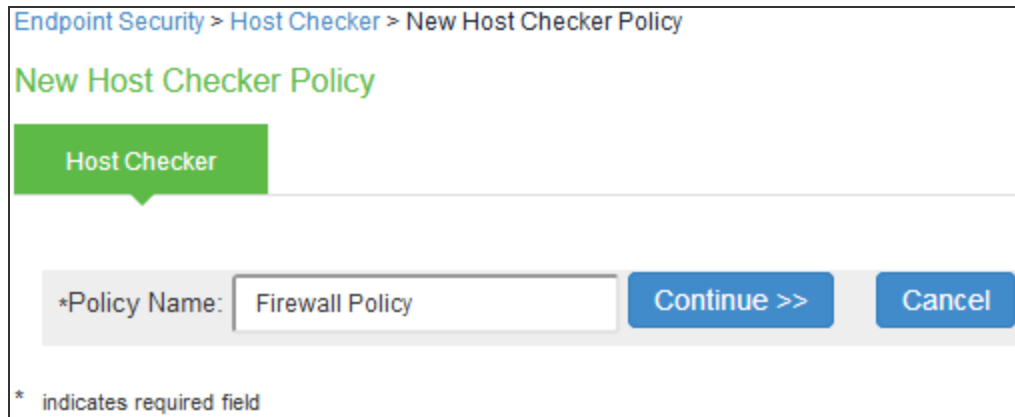
Restrict access to administrators only
Only administrator URLs will be accessible. Note that Administrators can attempt to sign in even if all rules on this page are disabled.
Warning: Enabling this option will immediately terminate all user sessions.

New URL... Delete... Enable Disable Save Changes

Administrator URLs	Sign-In Page	Authentication Realm(s)	Enabled
<input type="checkbox"/> */admin/	Default Sign-In Page	Admin Users	✓
User URLs	Sign-In Page	Authentication Realm(s)	Enabled
<input type="checkbox"/> */guestadmin/	Default Sign-In Page	Guest Admin (N/A)	✓
<input type="checkbox"/> */guest/	Default Sign-In Page	Guest (Guest)	✓
<input type="checkbox"/> */questsponsor/	Default Sign-In Page	Guest Sponsor (N/A)	✓

Creating a Host Checker Policy

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Under Policies, Click **New** and enter a policy name and click **Continue**.



Endpoint Security > Host Checker > New Host Checker Policy

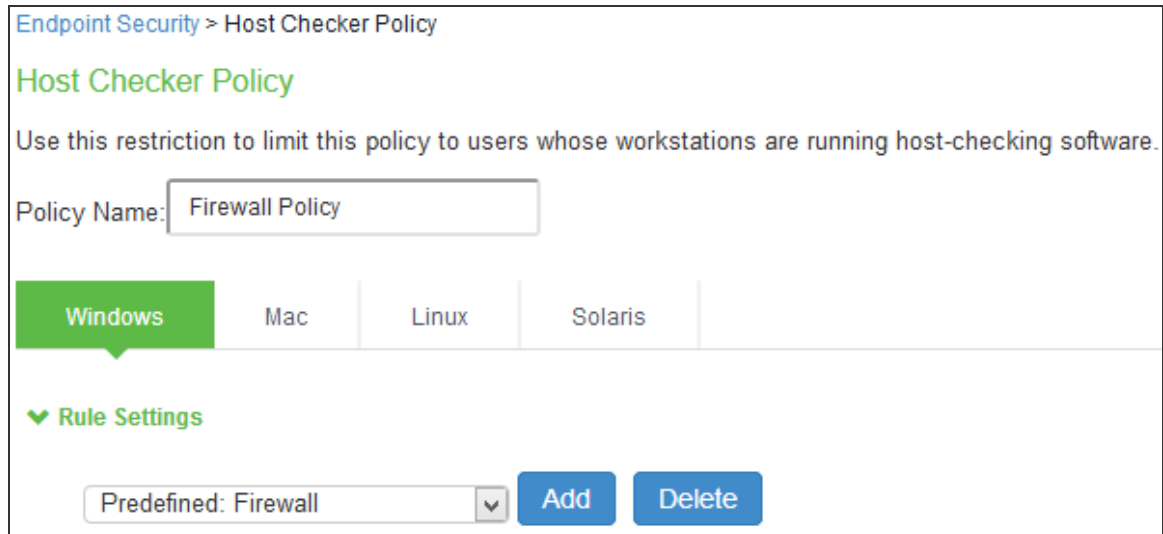
New Host Checker Policy

Host Checker

*Policy Name:

* indicates required field

3. Under Rule Settings, select the rule type as **Predefined Firewall** and click **Add**.



Endpoint Security > Host Checker Policy

Host Checker Policy

Use this restriction to limit this policy to users whose workstations are running host-checking software.

Policy Name:

Windows Mac Linux Solaris

▼ Rule Settings

- Enter the rule name and specify the criteria for compliance and click **Save Changes**.

Configuration > Host Checker Policy > Add Predefined Rule : Firewall

Add Predefined Rule : Firewall

Rule Type: Firewall

*Rule Name:

▼ *Criteria

Require any supported product.

Require specific products/vendors

Require any supported product from a specific vendor.

Available Vendors:

adaware
Agnitum Ltd.
AhnLab, Inc.
ALLIT Service, LLC.
Arcabit

Add ->

<- Remove

Selected Vendors:

Microsoft Corporation

Require specific products

▼ Optional

Monitor this rule for change in result

Note: Enabling this option will report change in compliance for this rule to the Pulse Policy Secure immediately. The client component requires additional computing cycles to report change in compliance immediately. We strongly recommend that this option be enabled for rules that are dynamic in nature, for example a rule for RTP check provided by AntiVirus software. For other rules the host checker update frequency should be used to get periodic health checks from endpoints.

▼ Remediation

Click on the remediation column headers to see the list of Firewalls supporting remediation

10 records per page

Search:

Product Name	Turn On Firewall	
Windows Firewall (10.x)	<input type="checkbox"/>	
Windows Firewall (6.x)	<input type="checkbox"/>	

← Previous 1 Next →

Powered by OPSWAT

Save Changes Cancel

* indicates required field

Creating User Roles

- Select **Users > User Roles > Guest Role (Default)**.



User defined roles can also be created. For example, Remediation Role.

2. Click **Save Changes**.

User Roles > Guest > General > Overview

Overview

General Enterprise Onboarding Agent Agentless

Overview Restrictions Session Options UI Options

* Name:

Description:

[Save Changes](#)

Options

If these settings are not specified by any roles assigned to the user, the settings specified in [Default Options](#) will be used.

Session Options [\(Edit\)](#)

UI Options [\(Edit\)](#)

Enable Guest User Account Management Rights

Enable Sponsored Guest User Account Management Rights

Cloud Application Visibility [\(Application Policies | Options\)](#)

Enterprise Device Onboarding

Check the 'Enterprise Onboarding' to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

Enterprise Onboarding [Options](#) (VPN, Wifi and Certificate Profiles)

[Save Changes](#)

* indicates required field

User Roles > Remediation > General > Overview

Overview

General Enterprise Onboarding Agent Agentless

Overview Restrictions Session Options UI Options

* Name:

Description:

[Save Changes](#)

Options

If these settings are not specified by any roles assigned to the user, the settings specified in [Default Options](#) will be used.

- Session Options [\(Edit\)](#)
- UI Options [\(Edit\)](#)
- Enable Guest User Account Management Rights
- Enable Sponsored Guest User Account Management Rights
- Cloud Application Visibility [\(Application Policies | Options\)](#)

Enterprise Device Onboarding

Check the 'Enterprise Onboarding' to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

- Enterprise Onboarding [Options](#) (VPN, Wifi and Certificate Profiles)

[Save Changes](#)

* indicates required field

3. Select **User Roles** > <**Full Access Role**> > **General** > **Restrictions** > **Host Checker**. Add the Firewall Policy restriction created earlier in [Creating a Host Checker Policy](#) for Full Access Role. Click **Save Changes**.

User Roles > FullAccessRole > General > Restrictions > Host Checker

Host Checker

General Agent Agentless

Overview Restrictions Session Options UI Options

Source IP Browser Certificate Host Checker

Allow all users (Host Checker not required)

Allow users whose workstations meet the requirements specified by these Host Checker policies:

Available Policies:

- Demo-SCCM-Policy
- TrendMicro AV
- HC NOTEPAD WIN

Add ->

Remove

Selected Policies:

- Firewall Policy

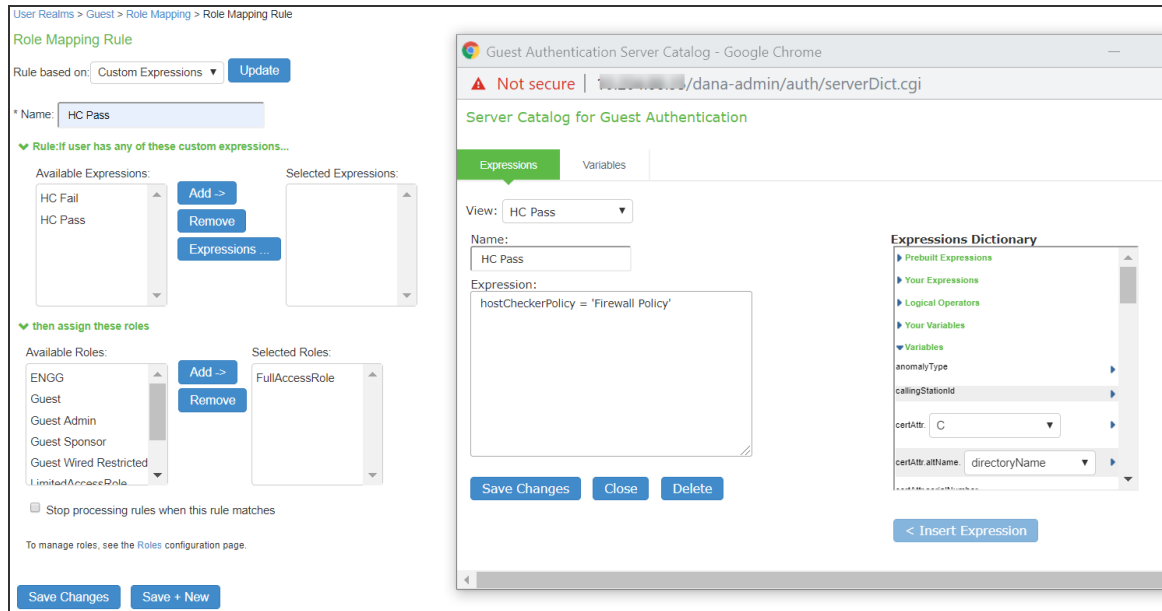
Allow access to the role if any **ONE** of the selected policies is passed.

To manage Host Checker policies, see the [Host Checker](#) configuration page.

Save Changes

For Remediation Role, ensure that the Host Checker not required option is not selected.

1. Set Role Mapping rules. Select **User Realms > Guest > Role Mapping > New Rule**.



Once the role mapping rules are configured the following screen is displayed.



Creating a new RADIUS Client

Add the Switch as RADIUS client

1. Select **Endpoint Policy > Network Access > RADIUS Client**.
2. Enter the name.
3. Enter the IP address of the Switch.
4. Select the make/model as Huawei.
5. Select the default location group as Guest.

- Click **Save Changes**.

Shared Secret will be used in the Huawei/RADIUS configuration.

Network Access > RADIUS Client > HUAWEI_WLC_RADIUS_CLIENT

HUAWEI_WLC_RADIUS_CLIENT

▼ RADIUS Client

* Name: HUAWEI_WLC_RADIUS_CLIENT Label to reference this RADIUS Client.

Description: Description of Radius Client for Adding Huawei WLC

* IP Address: IP Address of this RADIUS Client.

* IP Address Range: 1 Number of IP Addresses for this RADIUS Client

* Shared Secret: RADIUS shared secret

* Make/Model: Huawei To manage make/model, see the RADIUS Vendor

* Location Group: Guest To manage groups, see the Location Group

▼ Dynamic Authorization Support

Support Disconnect Messages Disconnect Message Support

Support CoA Messages Change of Authorization Message Support

*Dynamic Authorization Port: 3799 Dynamic Authorization Extensions Port

Save Changes

* indicates required field

Configuring RADIUS Return Attribute Policies

Define Radius Return Attribute policy based on ACL for different roles.

- Set RADIUS return attributes. Select **Endpoint Policy > Network Access > RADIUS Return Attribute Policies**. Click **New Policy**.

2. Under RADIUS Attributes tab, select the check box for **Return Attribute**. Select appropriate Vendor Specific Attribute as Return Attribute. In the Value field, define the ACL/Firewall Filter. For example, Return Attribute is *Filter-Id* and Value as *full_access.in*.

Network Access > Radius Attributes > RADIUS Return Attributes > Guest Access Policy

Guest Access Policy

General

* Name: Required: Label to reference this policy.

Description:

Location Group

Location Groups
Specify the Location Group for which this policy applies.

Available Location Groups:

Selected Location Groups:

Selected Radius Clients
Below list is populated dynamically based on the selected Location Groups

Vendor (Manufacturer)	Client Details
Huawei	HUAWEI_WLC_RADIUS_CLIENT

Access Control Policy Settings

Select below option to control the access level for the device/user connecting to the network

Provide full Access (Open Port) Note: Selecting this option will result in opening the port without any restrictions

Control the Access Note: Selecting this option enables control of the device or user access

Access can be controlled using the VLAN Id, ACLs and Radius Return Attribute settings below

Control using VLAN Id: (1 - 4094) Note: This option is used for assigning devices to corresponding VLAN on the switch

Specify the PPS interface to which end points will connect while they are assigned to above VLAN

Automatic Internal External

Control access using Access Control List (ACL) settings (Supported only for Cisco, Juniper, HP)

Control access using Radius Return Attributes Note: These attributes are sent to switch for controlling the access

Return Attribute	Radius Auth Server Attribute Value	Auth Server Catalog Attribute Value	Value	
<input type="text" value="Filter-Id"/>	<input type="text" value="-none-"/>	<input type="text" value="-none-"/>	<input type="text"/>	<input type="button" value="Add"/>
<input type="checkbox"/> <input type="text" value="Filter-Id"/>	<input type="text" value="-none-"/>	<input type="text" value="-none-"/>	<input type="text" value="full_access.in"/>	

Add Session-Timeout attribute Note: This will send session timeout attribute equal to session lifetime

Specify the action that needs to be taken for the device upon expiration of session timeout on the switch

Terminate the session Re-authenticate the session

Roles

Select the roles to which this policy is applicable

Any Role Selected below Other than selected below

Available roles:

Selected roles:

NOTE: Any changes to this page results in termination of existing L2 connections and triggers reconnections.

Similarly define a remediation policy with Return Attribute as **Filter-Id** and Value as **limited_access.in**.

Network Access > Radius Attributes > RADIUS Return Attributes > Limited Access Role

Limited Access Role

General

* Name: Required: Label to reference this policy.

Description:

Location Group

Specify the Location Group for which this policy applies.

Available Location Groups:

Selected Location Groups:

Selected Radius Clients
Below list is populated dynamically based on the selected Location Groups

Vendor (Manufacturer)	Client Details
Huawei	HUAWEI_WLC_RADIUS_CLIENT

Access Control Policy Settings

Select below option to control the access level for the device/user connecting to the network

Provide full Access (Open Port) Note: Selecting this option will result in opening the port without any restrictions

Control the Access Note: Selecting this option enables control of the device or user access

Access can be controlled using the VLAN Id, ACLs and Radius Return Attribute settings below

Control using VLAN Id: (1 - 4094) Note: This option is used for assigning devices to corresponding VLAN on the switch

Specify the PPS interface to which end points will connect while they are assigned to above VLAN

Automatic Internal External

Control access using Access Control List (ACL) settings (Supported only for Cisco, Juniper, HP)

Control access using Radius Return Attributes Note: These attributes are sent to switch for controlling the access

Return Attribute	Radius Auth Server Attribute Value	Auth Server Catalog Attribute Value	Value
<input type="text" value="Filter-Id"/>	<input type="text" value="-none-"/>	<input type="text" value="-none-"/>	<input type="text"/>
<input type="checkbox"/> Filter-Id	-none-	-none-	limited_access.in

Add Session-Timeout attribute Note: This will send session timeout attribute equal to session lifetime

Specify the action that needs to be taken for the device upon expiration of session timeout on the switch

Terminate the session Re-authenticate the session

Roles

Select the roles to which this policy is applicable

Any Role Selected below Other than selected below

Available roles:

Selected roles:

NOTE: Any changes to this page results in termination of existing L2 connections and triggers reconnections.

The following example shows the Filter-Id radius attribute policy for Huawei Switches.

Network Access > Radius Attributes > RADIUS Return Attributes

RADIUS Return Attributes

RADIUS Dictionary | RADIUS Vendor | Location Group | RADIUS Client | **RADIUS Attributes** | Network Infrastructure Device | SNMP Enforcement Policies

Return Attributes | Request Attributes | Attribute Logging

Show policies that apply to: All roles

A RADIUS return attributes policy specifies the return list attributes to send to an 802.1X network access device, such as which VLAN endpoints must use to access the network. If no policy applies, Open Port is the default action.

	Policies	ACL Settings	Attributes	Location Group	Interface	Applies to role
<input type="checkbox"/>	1. Limited Access Role This role will be applied when the guest endpoint does not meet the security policies	N/A	VLAN=201 Filter-Id=limited_access.in	Guest	AUTO	Remediation
<input type="checkbox"/>	2. Guest Access Policy This policy will be applied when Guest role is applied	N/A	VLAN=101 Filter-Id=full_access.in	Guest	AUTO	Guest

Keyboard shortcuts:
Use "←" and "→" keys to move selected items up and down (remember to click Save Changes after rearranging the list). Use **Ctrl+Plus** and **Ctrl+Minus** to expand and collapse all items.

The following example shows RADIUS return attribute used to send the VLAN ID. In the below example, VLAN 101 is sent for Guest Access Role and VLAN 201 for Limited Access Role.

The following example shows the Filter-Id radius attribute policy for Huawei Switches.



- When using VSAs there is no need to configure ACL/Firewall filters in the switches. These are managed by IPS and access control entries (ACEs) will be applied on the switches after User Authentication.
- VLAN change using CoA is supported with Huawei Switches.

Configuring Huawei WLC/Switch

Administrator must configure hw_redirect_url as redirect url parameter key and hw_login_url as key for the login url parameter on Huawei switch.

Configure external Port Authentication on Access Controller

Configure RADIUS authentication parameters.

Configure a RADIUS server template.

```
[Huawei]radius-server template radius_wlc_IPS
[Huawei-radius-radius_wlc_IPS]display this
radius-server template radius_wlc_IPS
radius-server shared-key cipher %^%#XX!84-3lJ~dR8X#p:-{0(TF+'=IOe<MG'BR2QrL&%^%#
radius-server authentication 192.168.10.11 1812 weight 80
radius-server accounting 192.168.10.11 1813 weight 80
```

```
calling-station-id mac-format hyphen-split mode2 uppercase
# Create an AAA scheme and set the authentication method to RADIUS.
[Huawei]aaa
[Huawei-aaa]authentication-scheme radius_wlc_IPS
[Huawei-aaa-authen-radius_wlc_IPS]display this
authentication-scheme radius_wlc_IPS
authentication-mode radius
# Configure a Portal server profile
[Huawei]portal https-redirect enable
[Huawei] portal web-authen-server https ssl-policy ssl_policy port 8443
[Huawei]interface LoopBack 0
[Huawei-LoopBack0]display this
interface LoopBack0
ip address 10.0.0.1 255.255.255.255
[Huawei]free-rule-template name default_free_rule
[Huawei-free-rule-default_free_rule]display this
free-rule 0 destination ip 10.0.0.1 mask 255.255.255.255
[Huawei]url-template name test
[Huawei-url-template-test]display this
url-template name test
#URL of the guest login page
url https://<IPS-IP>/guest
# Configure hw_redirect_url as redirect url parameter key and hw_login_url as key for the
login url parameter on Huawei.
# hw_redirect_url: URL that the user is redirected to after successful authentication.
# hw_login_url: Switch URL needed to post parameters. Admin must configure login url value.
url-parameter redirect-url hw_redirect_url login-url hw_login_url
https://10.0.0.1:8443/login
# https://10.0.0.1:8443/login is the login page of the Huawei
[Huawei]web-auth-server wlan-net
[Huawei-web-auth-server-wlan-net] display this
web-auth-server wlan-net
server-ip 192.168.10.11
port 50100
url-template test
server-detect action log
protocol http
http get-method enable
http-method post login-fail response err-msg authenserve-reply-message (or) http-
method post login-fail response err-msg msg AuthenticationFailed (Recommended to
configure one of this)
```

```
#Configure the Portal access profile portal_access_profile
    [Huawei-portal-acces-profile-portal_access_profile]display this
    portal-access-profile name portal_access_profile
    web-auth-server wlan-net direct

#Create the authentication profile wlan-authentication
    [Huawei-authen-profile-wlan-authentication]display this
    authentication-profile name wlan-authentication
    portal-access-profile portal_access_profile
    free-rule-template default_free_rule
    access-domain wlc_IPS dot1x
    access-domain wlc_IPS dot1x force
    access-domain wlc_IPS portal
    Configure WLAN service parameters.

# Create the security profile wlan-net and retain the default security policy (open system authentication).
    [Huawei]wlan
    [Huawei-wlan-view]security-profile name wlan-security

# Create the SSID profile.
    [Huawei-wlan-view]ssid-profile name wlan-ssid
    [Huawei-wlan-ssid-prof-wlan-ssid]display this
    ssid wlan-IPS

# Create the VAP profile wlan-vap, configure the data forwarding mode and service VLANs, and bind the security profile, authentication profile, and SSID profile to the VAP profile.
    [Huawei-wlan-view]vap-profile name wlan-vap
    [Huawei-wlan-vap-prof-wlan-vap]display this
    forward-mode tunnel
    service-vlan vlan-pool vlan_pool_101_201
    ssid-profile wlan-ssid
    security-profile wlan-security
    authentication-profile wlan-authentication

# Bind the VAP profile wlan-vap to the AP group and apply the profile to radio 0 and radio 1 of the AP.
    [Huawei-wlan-view]ap-group name ap-group1
    [Huawei-wlan-ap-group-ap-group1]display this
    regulatory-domain-profile domain1
    radio 0
    vap-profile wlan-vap wlan 1
    radio 1
    vap-profile wlan-vap wlan 1

#Create the ACL for full access and limited access. Admin must use the same ACL names in IPS.
    acl name full_access 3998
```

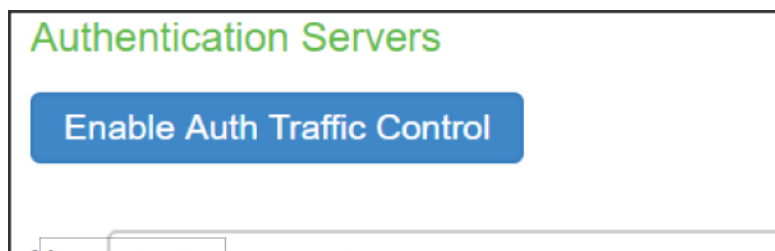
```
description full_access.in
rule 1 permit ip
acl name limited_access 3999
description limited_access.in
rule 1 deny ip destination <Resource-IP>
```

Example Configuration: Guest Access with Juniper Mist WLC

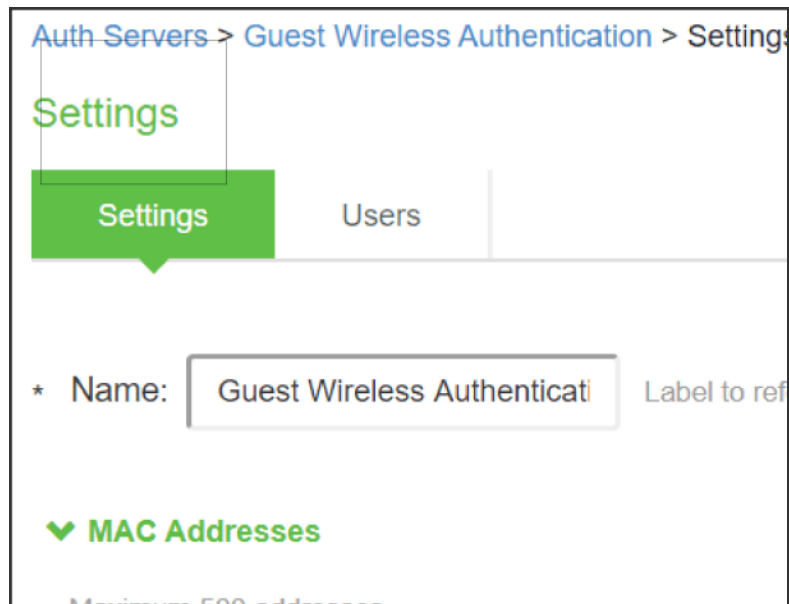
This section describes the configuration that is required on IPS to communicate with Juniper Mist WLC for Guest wireless authentication.

To configure IPS for guest wireless authentication:

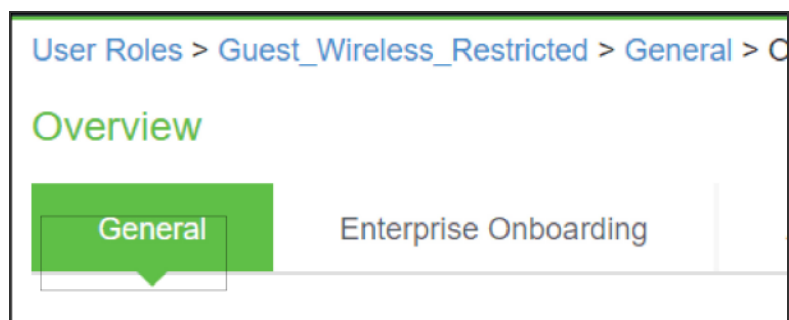
1. Select **Authentication > Auth.Servers**. The Authentication Servers screen appears. Use the Default Guest Wired Authentication Server.



2. Click Guest Wired Authentication available by default to view the settings.



3. You can make the necessary changes and click **Save Changes**.
4. Select Users > User Roles. The User Roles page appears.



5. Click Guest Wired Restricted user role available by default. The Agentless access is enabled for this role.

6. Select **Endpoint Policy > MAC Address Authentication Realms** and click Guest Wired authentication realm available by default.

7. Select **Endpoint Policy > Network Access > Location Group**. Select Guest Wired as MAC Auth Realm.
8. Configure the Mist WLC as a RADIUS client. Ensure that the Guest Wired location group and Support Disconnect Messages options are enabled.

- Configure the RADIUS return attributes for Guest Wired policy. Select **Endpoint Policy > Network Access > RADIUS Return Attribute Policies**. Click **New Policy**. Under RADIUS Attributes tab, select the check box for **Return Attribute**. The RADIUS return attributes are required for MAB authentication initially when the guest connects to the SSID (where the redirection happens) and then the session is bridged after the guest authenticates.

Supported Attributes: Filter-Id, Airspace-ACL-Name, Aruba-User-Role.

Cisco-AVPair is supported to set the redirection URL.

Tunnel-Private-Group-ID and Airespace-Interface-Name are used to assign the VLANs.

Policies	ACL Settings	Attributes	Location Group	Interface	Applies to role
1. Guest Wireless Radius Redirection Attributes User is given a Guest Wired Role when full authentication happens.	N/A	Cisco-AVPair=radius-redirec- ad=URL Cisco-AVPair=radius-redirec=170.99.78.28/guest?Cisco-Radius-Access-Config=radius-Tunnel-Private-Group-ID=74	Guest Wired	N/A	Guest Wired Restricted
2. Guest Radius Return Attributes User is given a Guest Role when Guest Wired L2 session and L3 browser session gets bridged.	N/A	Filter-Id=Full_Access Tunnel-Private-Group-ID=60	Guest Wired	N/A	Guest

Configuring Mist WLC

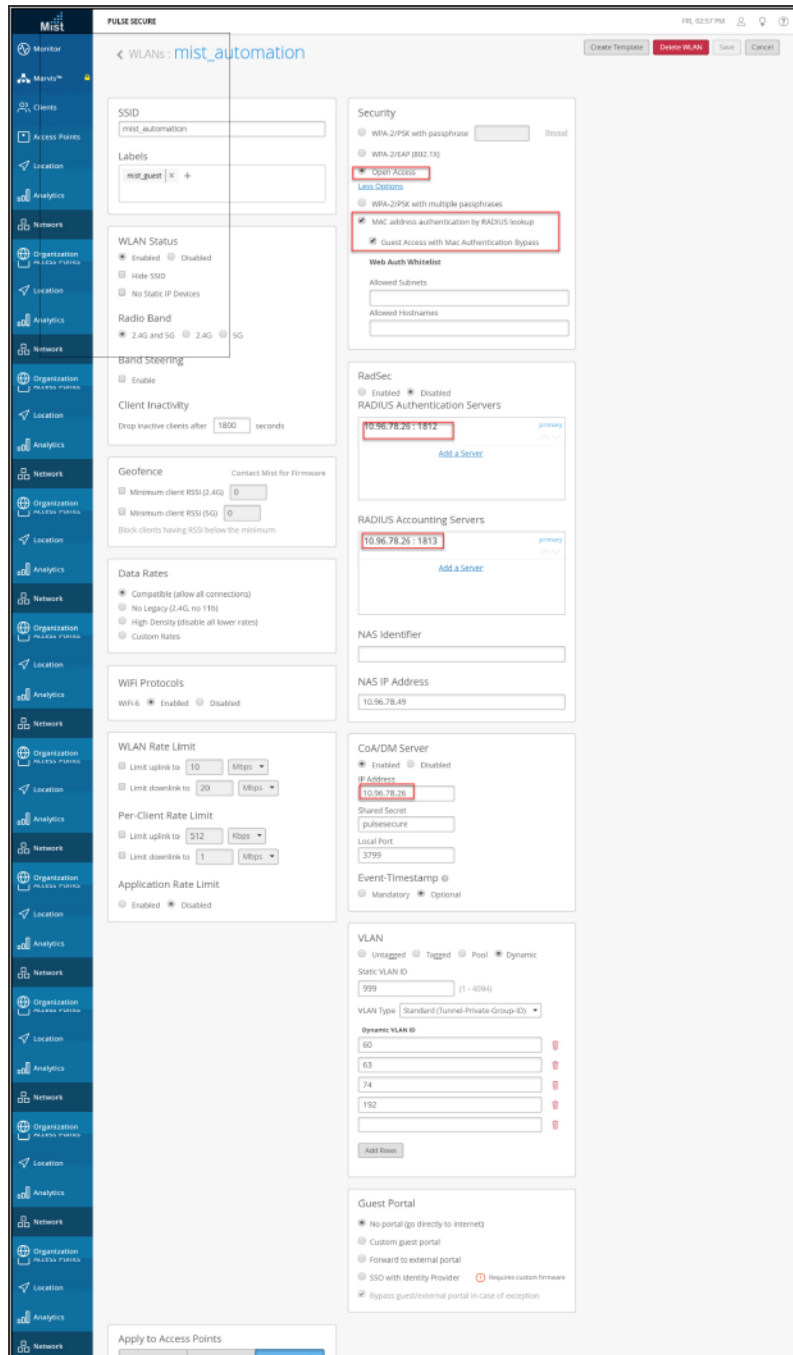
To configure WLAN on Mist:

- Add Mist as Access Point.

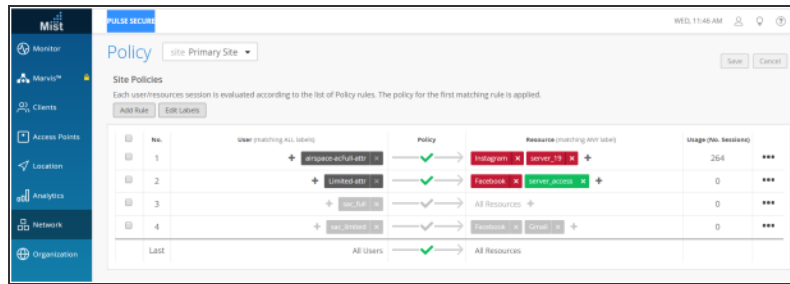
Status	Name	MAC Address	IP Address	No. Clients	Uptime	Total Bytes	Capabilities	VRF
Disconnected	0	0 B
Connected	Juniper_Mist_AP	1	2d 2h 58m	1.3 GB

- Setup the Wireless Networks, Select **Network > WLANs**. Click **Add WLAN**.
- Configure Name, SSID.
- Under Security, select **Open Access**.
- Enable **Guest Access with Mac Authentication Bypass**.

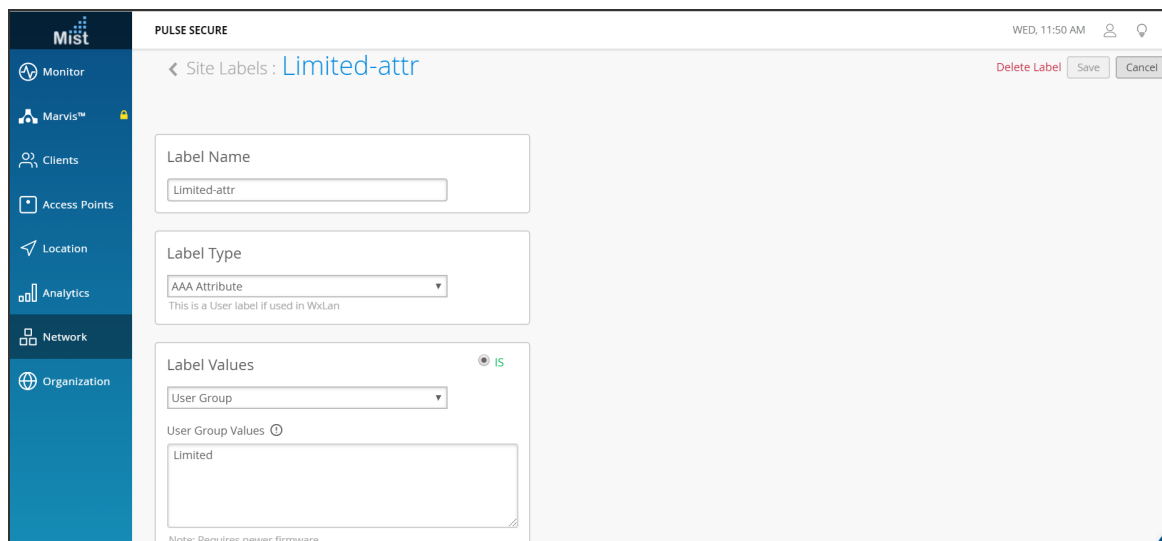
- Under RADIUS Authentication Server and RADIUS Accounting Server, specify the IPS IP address.



7. Create Security Policy to control resource access.



8. You can also issue a label. The label is used to form tags or groups, which can be used to create security policies.



Enterprise Onboarding

Overview

Ivanti Policy Secure(IPS) Enterprise Onboarding feature automatically configures and provisions mobile and personal devices running on platforms such as Windows, MAC OSX, Android, and iOS. It enables them to securely connect to the enterprise network in support for Bring Your Own Device (BYOD) initiatives.

The onboarding provides a way to configure Wireless, VPN, and device certificate profiles on a device. Using these profiles the users can securely connect to enterprise network and access enterprise resources. The profiles can be configured on a single IPSIPS server dedicated to onboarding or on each server.

The supported profiles depend on the device type and whether the Pulse Client is installed.

For enterprise onboarding a separate license called *"Advanced Mobile Licenses – Onboarding"* is required.

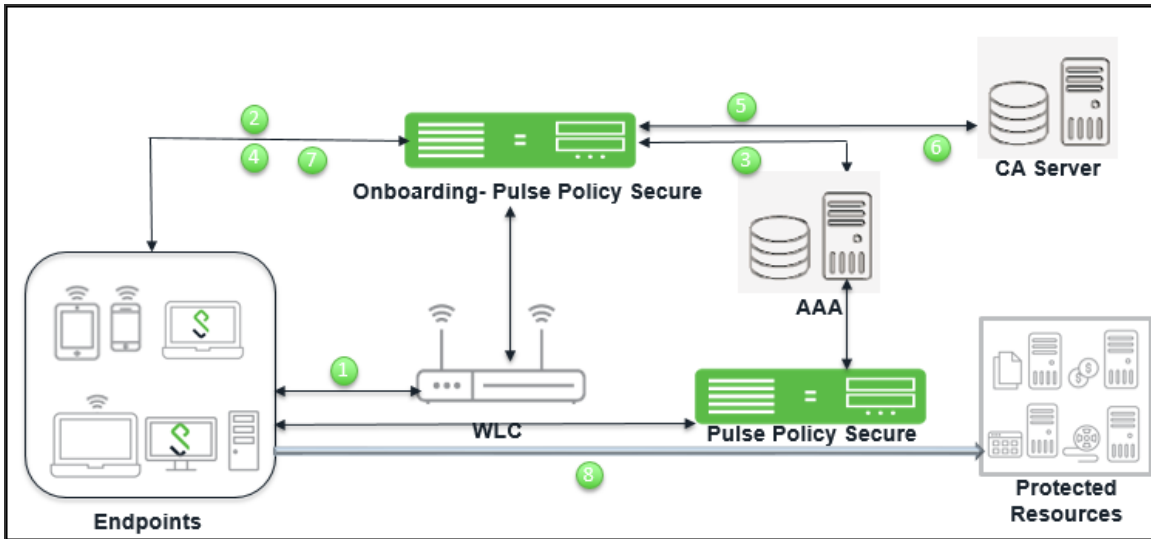
- Android platform supports all profiles. However, Pulse Client application must be installed during onboarding.
- iOS platform supports all profiles through Safari browser.
- Windows platform supports Wi-Fi and certificate profiles (IE, Firefox, or Chrome browser). The Pulse Client onboarding application must be installed during onboarding. Windows 8 RT and Windows 8 Phone are not supported.
- MAC OSx platform supports Wi-Fi and certificate profiles (Safari browser).

You can see more information on the supported platforms in the Supported Platform document.

You can also define the profiles on an external MDM server. If an external MDM server is used, the user will see a link and instructions on the onboarding page to continue onboarding. Onboarding is initiated from the browser.

Deployments

Enterprise Onboarding allows users to securely access enterprise network resources with any device. Wi-Fi, VPN and certificate profiles can be defined and downloaded to a device during onboarding, depending on the device type. The deployment diagram illustrates how a BYOD user can get onboarded through IPS to connect to enterprise network and access enterprise resources.



The workflow for enterprise onboarding is described below:

1. User tries to connect to enterprise network using the BYOD.
2. WLC is configured with Captive portal, which redirects the user to IPS login page where the devices can be onboarded.
3. User is authenticated through AAA framework.
4. User is provided with an onboarding link.
5. To generate and provision device certificate, IPS submits CSR to CA server.
6. CA server signs the CSR and sends the certificate to IPS.
7. Ivanti Policy Secure(IPS) pushes the configured profiles to devices.
8. User logs in and access the network.

Configuring Enterprise Onboarding

This section covers the configuration for enterprise onboarding. It involves configuring the profiles, SCEP server and CSR templates.

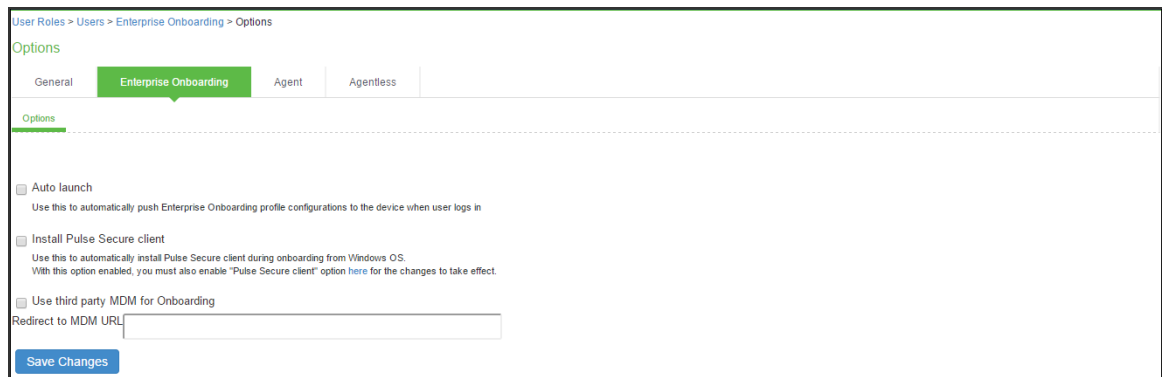
Configuring Enterprise Onboarding for a User Role

Enterprise onboarding is enabled in the user role, and each profile can be applied to all user roles or specific roles. The SCEP server and CSR templates allow certificates to be generated dynamically for device and server authentication.

To enable enterprise onboarding for a user role:

1. In the admin console, choose **Users > User Roles > RoleName > General > Overview**.
2. In the Enterprise Device Onboarding section, select the **Enterprise Onboarding** check box.
3. Click **Save Changes**.

- Click the **Enterprise Onboarding** tab or click **Options** next to the **Enterprise Onboarding** check box to specify the following:
 - Auto launch** – Displays the onboarding page when the user logs in to IPS if enterprise onboarding is enabled for the user's role (the default). If this option is disabled, an onboarding link is displayed on the home page.
 - Install Pulse Client** – Select this option to automatically install Pulse Client during windows onboarding.
 - Use third party MDM for onboarding** – Displays a link on the onboarding or home page where the user can download profiles from an MDM server. Enter the URL for the MDM page in the text box.



The screenshot shows the 'Options' configuration page for Enterprise Onboarding. The breadcrumb trail is 'User Roles > Users > Enterprise Onboarding > Options'. The 'Options' tab is selected, and the 'Enterprise Onboarding' sub-tab is active. The page contains three main options, each with a checkbox and a description:

- Auto launch**
Use this to automatically push Enterprise Onboarding profile configurations to the device when user logs in
- Install Pulse Secure client**
Use this to automatically install Pulse Secure client during onboarding from Windows OS.
With this option enabled, you must also enable "Pulse Secure client" option [here](#) for the changes to take effect.
- Use third party MDM for Onboarding**
Redirect to MDM URL:

A 'Save Changes' button is located at the bottom left of the form.

- Click **Save Changes**.

Configuring the SCEP Server

The Simple Certificate Enrollment Protocol (SCEP) server configuration and CSR templates allows each client device to dynamically obtain certificates for authentication. The SCEP server and CSR templates allow certificates to be generated dynamically for device and server authentication.

To define the SCEP server:

1. Select **Users > Enterprise Onboarding**.
2. Click **SCEP Configuration**.

Enterprise Onboarding > SCEP Configuration

SCEP Configuration

SCEP Configuration | CSR Templates | VPN Profiles | WiFi Profiles | Certificate Profiles

* SCEP Server URL: Example: http://<SCEP Server>/certsrv/mscep/mscep.dll for Microsoft Network Device Enrollment Service(NDES)

Challenge:

Retries: Shared secret for automatic enrollment
Number of retries when connection fails (0 - 10)

Retry Delay: Duration in seconds between successive retries (0 - 10)

Upload Encryption Certificate: No file chosen Used to encrypt the requests to SCEP Server
Manually upload the encryption certificate or run **Test Configuration** below with **Test Enrollment** to upload it automatically.

Current Certificate: Issued To:
Issued By:
Valid:
Details: [Other Certificate Details](#)

Test Connectivity
 Test Enrollment

3. Complete the configuration as described below.

Setting	Description
SCEP Server URL	Enter the URL for a SCEP server. The following SCEP servers are supported: Microsoft AD 2008 Symantec mPKI
Challenge	Specify the password required by the SCEP server.
Retries	Specify the number of attempts to access the server when the first attempt fails.
Retry Delay	Specify the number of seconds between retry attempts.
Upload Encryption Certificate	Click Browse to upload the certificate used to encrypt SCEP requests. To upload the certificate automatically, select the Test Enrollment check box, select a CSR template, and click Test Configuration .

4. Click **Save Changes**.

Configuring CSR Templates

If the SCEP server is configured, the Certificate Signing Request (CSR) templates can be used in the VPN, Wi-Fi, and certificate profiles to allow each onboarded device to dynamically obtain certificates for authentication on iOS devices. Up to 10 templates can be defined.




All LDAP attributes (such as **<ldap.userAttrName>**) and variables (such as **<user>**) can be used in the Subject DN, Email, and Subject Alternative Name Value fields. However, if you enter an LDAP variable with a string vector data type in the Subject Alternative Name Value field, only the first value in the string will be used.

To configure CSR templates:

1. In the admin console, choose **Users > Enterprise Onboarding > CSR Templates**.
2. To add a template, click **New CSR Template** or select an existing template that you want to change, duplicate, or delete. Clicking **Duplicate** creates a copy of the selected template with Copy of before the template name.

The screenshot shows the 'New Certificate Signing Request Template' form. The breadcrumb is 'Enterprise Onboarding > CSR Templates > New Certificate Signing Request Template'. The form title is 'New Certificate Signing Request Template'. The fields are: '* Name:' (text input), '* Subject DN:' (text input with example 'CN=<USERNAME>,OU=Employees,O=Company'), 'Email:' (text input), 'Subject Alternative Name Type:' (dropdown menu set to 'None'), 'Subject Alternative Name Value:' (text input), and 'Key Size:' (dropdown menu set to '2048-bit'). A 'Save Changes' button is at the bottom left. A note at the bottom right says 'Ensure that the selected Key Size is enabled on the SCEP Server. An invalid Key Size will cause a certificate request failure.' A footnote at the bottom left says '* indicates required field'.

3. Specify the following information:

Setting	Description
Name	Specify the template name displayed in the list of CSR templates.
Subject DN	Specify the subject distinguished name. For example: CN=<USERNAME>,OU=Engineering,O=Comp All LDAP attributes (such as <ldap.userAttrName>) and variables (such as <user>) can be used.
Email	(Optional) Specify an email address with the <USER> variable, such as <USER>@sample.net .
Subject Alternative Name Type	Select an alternative name type if the CA requires an alternative subject name. The types include RFC-822 Name (an e-mail address), DNS domain name, URI, and IP address.
Subject Alternative Name Value	Specify one or more values for the selected alternative name type. Multiple values must be separated by a comma or space.  If an LDAP variable is specified that has a string vector data type, only the first value in the string will be used.
Key Size	Select the key size used by the SCEP server.

4. Click **Save Changes**.

Configuring VPN Profiles

VPN profiles provide Android and iOS devices with secure access to enterprise networks. One or more VPN profiles can be assigned to specific user roles or to all roles. Up to 10 profiles can be defined.



All LDAP attributes (such as **<ldap.userAttrName>**) and variables (such as **<user>**) can be used in the Username, Realm, and Role fields.

To define VPN profiles:

1. In the admin console, choose **Users > Enterprise Onboarding > VPN Profiles**.
2. To add a profile, click **New Profile** or select an existing profile that you want to change, duplicate, or delete. Clicking **Duplicate** creates a copy of the selected profile with **Copy of before the profile name**.
3. The first profile that matches a user's role and client type becomes the default VPN profile on the client. Use the arrow keys to move a profile up or down the list.

The screenshot shows the 'New VPN Profile' configuration page. The breadcrumb trail is 'Enterprise Onboarding > VPN Profiles > New VPN Profile'. The page title is 'New VPN Profile'. The form includes the following fields and options:

- *Name:** A text input field with a placeholder character '|'. A note says 'Label to reference this profile.'
- Description:** A larger text input area.
- Apply to Client Types:** Two checked checkboxes for 'IOS' and 'Android'.
- *Server URL:** A text input field containing 'https://'. A note says 'Should start with https://'.
- Realm:** A text input field.
- Role:** A text input field.
- Username:** A text input field.
- Authentication Method:** Two radio buttons: 'Password' (selected) and 'Certificate'.
- Roles:** A section with a dropdown arrow. It contains a note: ''Enterprise Onboarding' in the Role must be enabled in order for this policy to take effect.' Below this are three radio buttons:
 - Policy applies to ALL roles
 - Policy applies to SELECTED roles
 - Policy applies to all roles OTHER THAN those selected below
- Available roles:** A list box containing 'Guest', 'Guest Admin', and 'Users'. It has an 'Add ->' button.
- Selected roles:** A list box containing '(none)'. It has a 'Remove' button.
- Save Changes:** A blue button at the bottom left.

4. Specify the following profile information:

Setting	Description
Name	Specify the name to be displayed in the list of VPN profiles.
Description	(Optional) Enter a description of the VPN profile.
Apply to Client Types	Select the device types the profile applies to (Android and iOS only).
Server URL	Specify the URL of the VPN server (must be a IPS device).
Realm	Specify the realm name. The realm is required only if the sign-in URL has the User picks from a list of authentication realms option enabled.
Role	Specify the user role. The user role is required if the role mapping rules for the user realm specify multiple roles and the User must select from among assigned roles option is enabled.
Username	Specify the <USER> variable for the user name.

Setting	Description
Authentication Method	<p>Select Password or Certificate for the user authentication method. For certificate authentication, specify the following:</p> <ul style="list-style-type: none"> • Use CSR Template—Select the CSR template used to obtain the certificate. To create a CSR template, see “Defining CSR Templates”. <XREF> • Enable VPN On Demand—Select this option to allow iOS devices to establish the VPN when a specific host or domain is accessed. To specify the first host or domain: • Match Domain or Host—Enter a hostname or a partial domain name. For example, if you enter example.com, a match occurs when the user accesses any domain that ends with example.com, such as www.test-example.com. • On Demand Action—When a match occurs on the specified host or domain, select whether a VPN is always established, never established, or only if the DNS look-up fails (Establish If Needed). Selecting Never Establish does not prevent an existing VPN from being used. <p>To add another domain, click the + button. To remove a domain, select the check box next to the domain and click the - button. Up to 10 domains can be defined.</p>
Roles	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Policy applies to ALL roles—To apply this profile to all users. • Policy applies to SELECTED roles—To apply this profile only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list. • Policy applies to all roles OTHER THAN those selected below—To apply this profile to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.

5. Click **Save Changes**.

Configuring Wi-Fi Profiles

Wi-Fi profiles provide Android, iOS, MAC OS X, and Windows devices with secure access to wireless networks. One or more Wi-Fi profiles can be assigned to specific user roles or to all roles. Up to 10 profiles can be defined.

i All LDAP attributes (such as <ldap.userAttrName>) and variables (such as <user>) can be used in the Username and Password fields for the WPA Enterprise and WPA2 Enterprise security types.

To define Wi-Fi profiles:

1. In the admin console, choose **Users > Enterprise Onboarding > WiFi Profiles**.
2. To add a profile, click **New Profile** or select an existing profile that you want to change, duplicate, or delete. Clicking **Duplicate** creates a copy of the selected profile with **Copy of** before the profile name.

Enterprise Onboarding > WiFi Profiles > New WiFi Profile

New Wifi Profile

* Name: Label to reference this profile.

Description:

Apply to Client Types: iOS Android Mac OS X Windows

* SSID: SSID of the WiFi Network.

Non-Broadcast SSID:

Auto Connect: Not applicable for Android clients.

Security Type:

Roles

'Enterprise Onboarding' in the Role must be enabled in order for this policy to take effect.

Policy applies to ALL roles

Policy applies to SELECTED roles

Policy applies to all roles OTHER THAN those selected below

Available roles:


Selected roles:

*Indicates required field


3. Specify the following profile information:

Setting	Description
Name	Specify the name to be displayed in the list of Wi-Fi profiles.
Description	(Optional) Enter a description of the profile.
Apply to Client Types	Select the device types the profile applies to (Android, iOS, MAC OS X, and Windows).
SSID	Specify the server set ID of the wireless network.
Non-Broadcast SSID	Select the check box if the wireless network does not broadcast its identity.
Auto Connect	Select the check box to connect the client automatically when the network is detected (not supported by Android clients).

Setting	Description
Security Type	<p>Select the type of authentication used by the network, and specify the password or enterprise settings, as required:</p> <ul style="list-style-type: none"> • None—No authentication required. • WEP—Wired Equivalent Privacy used for a non-enterprise network. Enter the network shared key in the displayed text box. • WPA Personal or WPA2 Personal—Wi-Fi Protected Access used for a non-enterprise network. You can select the encryption method (AES or TKIP) and enter the network shared key in the displayed text box (applies to Windows clients only). • WPA Enterprise or WPA2 Enterprise—Wi-Fi Protected Access used for an enterprise network. Select the Extensible Authentication Protocols (EAP) supported by the network’s RADIUS authentication server. <p>For Android devices, note the following:</p> <ul style="list-style-type: none"> • Android 4.3 or later is required • For the EAP-TLS protocol, the CA certificate must be configured (along with the client certificate) on Samsung devices for authentication. • An 802.1x RADIUS server certificate must be signed by a private root CA. Authentication fails if the certificate is signed by an intermediate root CA.

Setting	Description
EAP	<p>For the WPA Enterprise and WPA2 Enterprise security types, select the supported EAP protocols and specify the associated authentication settings:</p> <ul style="list-style-type: none">• None—If none of the EAP protocols is selected (Android devices only), enter the <USER> and <PASSWORD> variables in the Username and Password fields. <hr/> <p> iOS, MAC OS X, and Windows clients require at least one of the EAP types to be selected (PEAP, EAP-TLS, or EAP-TTLS).</p> <hr/>

Setting	Description
PEAP	<p>The PEAP protocol is supported by all clients. Specify the following:</p> <ul style="list-style-type: none"> • Inner Authentication Method—Select the protocol used to authenticate the username and password (None or MSCHAPv2). The None option is valid only for Android devices. • Username and Password—Enter the <USER> and <PASSWORD> variables. • Outer Identity—Specify an alternate username to be used outside the encrypted tunnel, such as anonymous, to conceal the user's identity in unencrypted packets. • Trusted Server Name(s)—Specify the IP address or fully qualified domain name of one or more trusted RADIUS servers used by the network. Multiple servers must be separated by a semicolon. • Trusted CA Certificate—For Windows clients, select the Trusted Root CA of the RADIUS server certificate, even if the device certificate is signed by an intermediate CA. The Trusted Root CA must be configured in a certificate profile before it can be selected here (see "Defining Certificate Profiles")<XREF>. <p>For iOS, MAC OS X, and Android clients, if the RADIUS server certificate is signed by an intermediate CA, create a certificate profile for the intermediate CA, and then select the certificate here. The certificate profile ensures that the intermediate CA is downloaded to the client.</p>

Setting	Description
EAP-TLS	<p>The EAP-TLS protocol is supported by all clients. Specify the following:</p> <ul style="list-style-type: none"> • Username—Enter the <USER> variable. • Use CSR Template—Select the CSR template used to obtain the certificate. To create a CSR template, see “Defining CSR Templates”.<XREF> • Trusted Server Name(s)—Specify the IP address or fully qualified domain name of one or more trusted RADIUS servers used by the network. Multiple servers must be separated by a semicolon. • Trusted CA Certificate—For Windows clients, select the Trusted Root CA of the RADIUS server certificate, even if the device certificate is signed by an intermediate CA. The Trusted Root CA must be configured in a certificate profile before it can be selected here (see “Defining Certificate Profiles”)<XREF>. <hr/> <p> On Windows 7 clients that have multiple certificates, users are prompted to select the certificate for 802.1x connections that use EAP-TLS.</p> <hr/> <p>For iOS, MAC OS X, and Android, if the RADIUS server certificate is signed by an intermediate CA, create a certificate profile for the intermediate CA, and then select the certificate here. The certificate profile ensures that the intermediate CA is downloaded to the client.</p>

Setting	Description
EAP-TTLS	<p>The TTLS protocol is supported by all clients. Specify the following:</p> <ul style="list-style-type: none"> • Inner Authentication Method—Select the protocol used to authenticate the username and password (None, PAP, or MSCHAPv2). The None option is valid only for Android devices. • Username and Password—Enter the <USER> and <PASSWORD> variables. • Outer Identity—Specify an alternate username to be used outside the encrypted tunnel, such as anonymous, to conceal the user's identity in unencrypted packets. • Trusted Server Name(s)—Specify the IP address or fully qualified domain name of one or more trusted RADIUS servers used by the network. Multiple servers must be separated by a semicolon. • Trusted CA Certificate—For Windows clients, select the Trusted Root CA of the RADIUS server certificate, even if the device certificate is signed by an intermediate CA. The Trusted Root CA must be configured in a certificate profile before it can be selected here (see "Defining Certificate Profiles")<XREF>. Also, if the RADIUS server certificate is signed by an intermediate CA, then the public intermediate CA must be configured in a certificate profile to ensure that the intermediate CA is downloaded to the client along with the Wi-Fi TTLS profile configuration. <p>For iOS, MAC OS X, and Android clients, if the RADIUS server certificate is signed by an intermediate CA, create a certificate profile for the intermediate CA, and then select the certificate here. The certificate profile ensures that the intermediate CA is downloaded to the client.</p>

Setting	Description
Roles	Select one of the following options: <ul style="list-style-type: none"> • Policy applies to ALL roles—To apply this profile to all users. • Policy applies to SELECTED roles—To apply this profile only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list. • Policy applies to all roles OTHER THAN those selected below—To apply this profile to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.

4. Click **Save Changes**.

Configuring Certificate Profiles



Certificate profiles specify the device certificates sent to each client device during onboarding. Up to 10 profiles can be defined.

For security reasons, certificate profiles cannot be included in the XML export or import.

To define certificate profiles:

1. In the admin console, choose **Users > Enterprise Onboarding > Certificate Profiles**.
2. To add a profile, click **New Profile** or select an existing profile that you want to change, duplicate, or delete. Clicking **Duplicate** creates a copy of the selected profile with Copy of before the profile name.

The screenshot shows the 'New Certificate Profile' form in the Enterprise Onboarding admin console. The breadcrumb trail is 'Enterprise Onboarding > Certificate Profiles > New Certificate Profile'. The form title is 'New Certificate Profile'. It includes a 'Name' field with a placeholder 'Label to reference this profile.', a 'Description' text area, and 'Apply to Client Types' checkboxes for iOS, Android, Mac OS X, and Windows. There are three radio button options for certificate generation: 'Import and Use Global Certificate', 'Import and Use CA Certificate', and 'Generate per User Certificate'. A 'Roles' section is expanded, showing a note that 'Enterprise Onboarding' in the role must be enabled. It offers three radio button options: 'Policy applies to ALL roles', 'Policy applies to SELECTED roles', and 'Policy applies to all roles OTHER THAN those selected below'. Below this, there are two lists: 'Available roles' (Guest, Guest Admin, Users) and 'Selected roles' (none), with 'Add ->' and 'Remove' buttons between them. A 'Save Changes' button is at the bottom left.

3. Specify the following information:

Setting	Description
Client Types	Select the device types the profile applies to (Android, iOS, MAC OS X, and Windows).
Import and Use Global Certificate	Select this option to use the IPS global certificate to authenticate the client device. Click Import Certificate & Key , click Browse to locate the certificate file, and then click Import. For more information about device certificates, see "Using Device Certificates".
Import and Use CA Certificate	Select this option to import any CA certificate (public Root CA, private Root, public intermediate CA, or private intermediate CA). These CA's can be used in Wi-Fi profiles and must be downloaded to the client devices. Click Import and Use CA Certificate , click Browse to locate the certificate, and then click Import CA Certificate .
Generate per User Certificate	Select this option to use the SCEP server and a CSR template to generate a certificate for each client. Select a CSR template from the Use Certificate Template list. To create a CSR template, see "Defining CSR Templates" <XREF>.
Roles	Select one of the following options: <ul style="list-style-type: none"> • Policy applies to ALL roles—To apply this profile to all users. • Policy applies to SELECTED roles—To apply this profile only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list. • Policy applies to all roles OTHER THAN those selected below—To apply this profile to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.

4. Click **Save Changes**.

Viewing Onboarded Devices

The Device Management page lists the following types of devices:

Onboarded devices— Devices that have Enterprise Onboarding enabled in the user’s role and have been onboarded during device registration. After a device is onboarded, it is displayed on the Device Management page until it is deleted.

The username, user roles, operating system, and registration date are shown for each device, along with the onboarded, and access status. Devices that become inactive or invalid must be deleted manually.

To view the Device Management page:

1. Select **System > Status > Devices**.
2. Use the controls described in table to view and manage the devices in the Device Management page.

Buttons	Administrative Actions	
Update	<p>To view a specific user, enter the username in the Show Users Named box and click Update. If you do not know the exact username, use an asterisk (*) as a wildcard character.</p> <p>To change the number of displayed devices, enter a number in the Show N devices box and click Update.</p> <p>To change the sort, click a column header.</p>	To refresh the page, click Update.
Delete	<p>To delete one or more devices, select the check box next to the appropriate devices and click Delete. If an onboarded device is deleted in error, the user must re-onboard the device.</p> <p>ActiveSync-only devices that are deleted in error are added automatically by the next ActiveSync.</p>	

Buttons	Administrative Actions	
Delete All	To delete the all devices, click Delete All.	

Troubleshooting

You can use the following message IDs in the user access log for troubleshooting:

- AUT31186—Indicates the status of an onboarding attempt (failed or successful)
- AUT31152—Indicates onboarding failed because the maximum device limit of 10000 has been reached
- AUT31187—Indicates the attempt to build a configuration profile failed due to an error
- AUT31188—Indicates a configuration profile was generated successfully, and lists the names of the profiles contained in the configuration profile

The following message IDs are related to device limits:

- SYS31177—Indicates the number of devices onboarded is nearing the system limit of 10000.
- SYS31178—Indicates the number of devices onboarded has exceeded the system limit of 10000 (critical error)
- SYS31193—Information message generated by a background process that attempts to delete device records when 95% of system limit (10000) is reached. It displays the number of device records deleted, the current number of onboarded devices, and the system limit.



If profile generation in the server is successful, but it fails in the client while installing, then the client logs should be analysed for the failure.

Clustering

Overview

A Ivanti Policy Secure(IPS) cluster is a group of IPS devices that act like a single IPS device, which enables high availability, load balancing and parallel processing. A IPS cluster pair is used to refer to a cluster of two IPS devices and a multiunit IPS cluster refers to a cluster of more than two IPS devices.

Clustering provides the following benefits:

- Load balancing- It refers to efficiently distributing the incoming request across a group of IPS devices. It optimizes resource usage, maximizes throughput, minimizes response time, and avoids overload of any single device.
- High Availability (HA)- It provides increased availability and enables uninterrupted access to data even if one of the devices fails.

Deployments

Ivanti Policy Secure(IPS) supports two types of cluster deployments:

- Deployment of Active/Active Cluster
- Deployment of Active/Passive Cluster

Requirements and Limitations

The following are the requirements and limitations for clustering:

- Cluster members must run the same software version.
- Cluster members must use the same hardware platform.
- State synchronization must occur only through the internal Network Interface Card (NIC). Ensure the cluster communication and resource access must take place over an internal network.
- You can deploy active/active or active/passive clustering only within the same IP subnet.



We recommend you to use Pulse One instead of cluster to sync only the configuration across devices.

Deployment of Active/Active Cluster

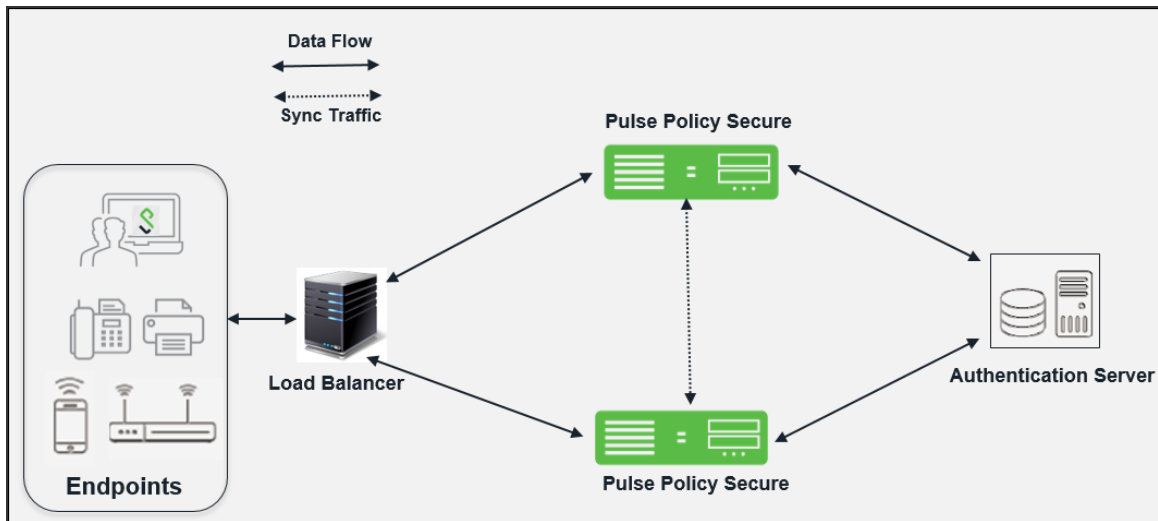
An Active/Active deployment provides load balancing and high availability. IPS relies on an external load balancer for distributing the load among IPS nodes. Active/Active cluster configuration allows increased aggregate system throughput; however, it does not provide increased scalability beyond the total licensed users. It also provides seamless failover, which is achieved by state synchronization between the devices.

If a node goes offline, the load balancer adjusts the load on the active nodes. Users do not need to sign in again, however some session information entered a few seconds before the active machine went offline, such as cookies and passwords, may not have been synchronized on the current device, in which case users may need to sign in again.

- WAN clustering is not supported.



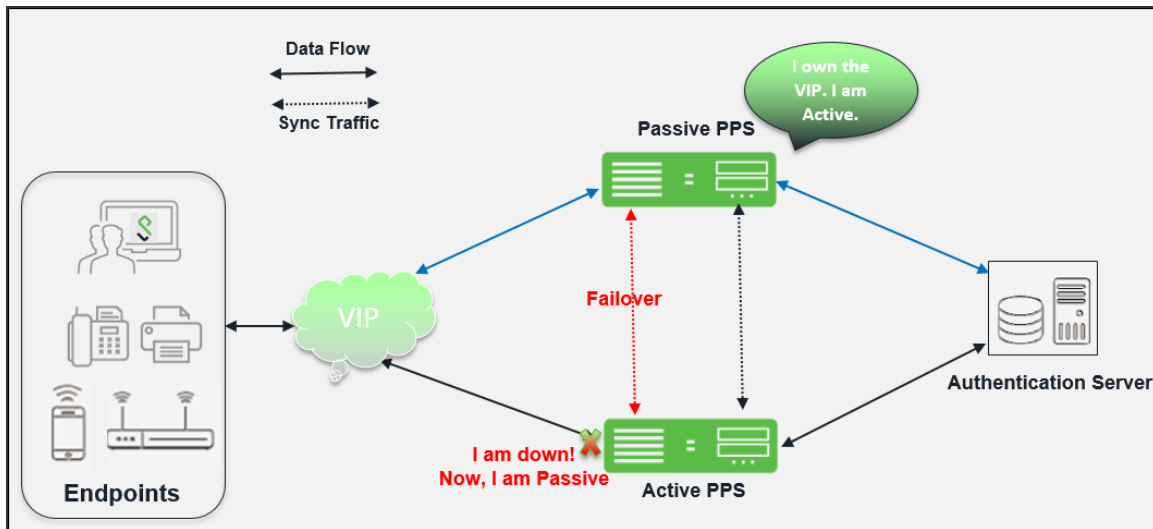
- You can deploy up to 8 nodes for PSA-7000. All other platform models support 2 node clusters only. The system (UI) allows adding up to 8 nodes. However, only up to 4 nodes in a cluster have been officially qualified.



Deployment of Active/Passive Cluster

An active/passive cluster configuration provides high availability. Active/Passive deployment allows seamless failover without the need to set up any external equipment. The states are synchronized between the two devices for all the configurations so that the devices are virtually identical.

Active/Passive clustering is supported only if the members of the cluster pair are in the same subnet because the VIP address must be shared by both the members. IPS uses a virtual IP (VIP) address to address the cluster pair in addition to addressing each device. The IP address takeover (IPAT) approach is used for the VIP address. If the active node fails, the passive node takes over the VIP address and sends a gratuitous Address Resolution Protocol (ARP) message notifying other networking devices that it now owns the VIP address. You should check that other devices in your network, especially the next-hop gateways, will consider the gratuitous ARP messages.



Cluster Configuration

Admin UI Configuration

Creating a Cluster

To create a cluster:

1. Select **System > Clustering > Create Cluster**.

Clustering > Create New Cluster

Create New Cluster

Join **Create**

Type: PSA-7000c

Cluster Name: Name of the cluster to create.
Must be alphanumeric, "-", or "_"; must start with a letter and have a maximum of 19 characters.

Cluster Password: Shared secret among the nodes in the cluster.
Must be at least 6 characters long

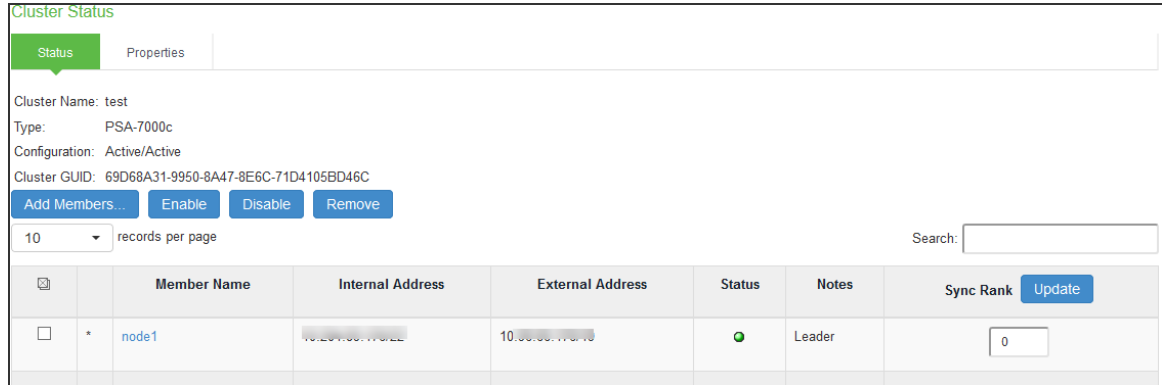
Confirm Password: Shared secret among the nodes in the cluster.
Must match the password you typed in the previous line

Member Name: Name of this node in the cluster
Must be alphanumeric, "-", or "_"; must start with a letter and have a maximum of 19 characters.

Create Cluster

Settings	Actions
Cluster Name	Specifies a name to identify the cluster.
Cluster Password	Specifies the cluster password. You need to enter the password again when specifying additional nodes to join the cluster. All nodes in the cluster use this password to communicate.
Confirm Password	Specifies the password that is confirmed.
Member Name	Specifies the name of this node in the cluster.

- Click Create Cluster. When prompted to confirm the cluster creation, click Create. After the device initializes the cluster, the Clustering page displays the Status and Properties tabs.



The screenshot shows the 'Cluster Status' page with two tabs: 'Status' (active) and 'Properties'. The cluster details are as follows:

- Cluster Name: test
- Type: PSA-7000c
- Configuration: Active/Active
- Cluster GUID: 69D68A31-9950-8A47-8E6C-71D4105BD46C

Below the details are four buttons: 'Add Members...', 'Enable', 'Disable', and 'Remove'. A dropdown menu shows '10 records per page' and a search box is present.

	Member Name	Internal Address	External Address	Status	Notes	Sync Rank	Update
<input type="checkbox"/>	* node1	10.0.0.100	10.0.0.100	●	Leader	0	

Configuring an Active/Active or Active/Passive Cluster

Once the cluster is created, you can modify the cluster properties to configure the cluster as an Active/Passive cluster. The cluster is created as an Active/Active cluster by default.

i If IPv6 is required, then configure both the nodes with IPv6 settings before creating the cluster.

To configure the cluster properties:

1. Click Properties tab of the cluster.

Clustering > Cluster Properties

Cluster Properties

Status **Properties**

Type: PSA-7000c

Cluster Name:

Cluster Password:

Confirm Password:

▼ Configuration Settings

Active/Passive configuration
This is a high-availability failover mode, in which one node is active while the other is held as backup.

Internal VIP:

IPv4: IPv6:

External VIP:

IPv4: IPv6:

Active/Active configuration

▼ Synchronization Settings

Synchronize log messages

Synchronize last access time for user sessions

▼ Network Healthcheck Settings

Number of ARP Ping failures before interface is disabled (should be greater than 0):


Disable external interface when internal interface fails

▼ Advanced Settings

Enable Advanced Settings

2. Complete the configuration as described in the following table. Active/Active configuration is selected by default.

Settings	Actions
Cluster Name	Identifies the cluster.
Configuration Settings	
Active/Passive configuration	Runs a cluster pair in active/passive mode. Then specify an internal VIP (virtual IP address) and an external VIP if the external port is enabled.
Active/Active configuration	(Default) Runs a cluster pair in active/active mode. This configuration runs a cluster of two or more nodes in active/active mode using an external load balancer. To change a two-unit active/passive cluster to an active/active cluster with more than two nodes, first change the configuration of the two-unit cluster to active/active and then add the additional nodes.
Synchronization Settings	
Synchronize log messages	Propagates all log messages among the devices in the cluster.
Synchronize last access time for user sessions	Propagates the latest user access information across the cluster.

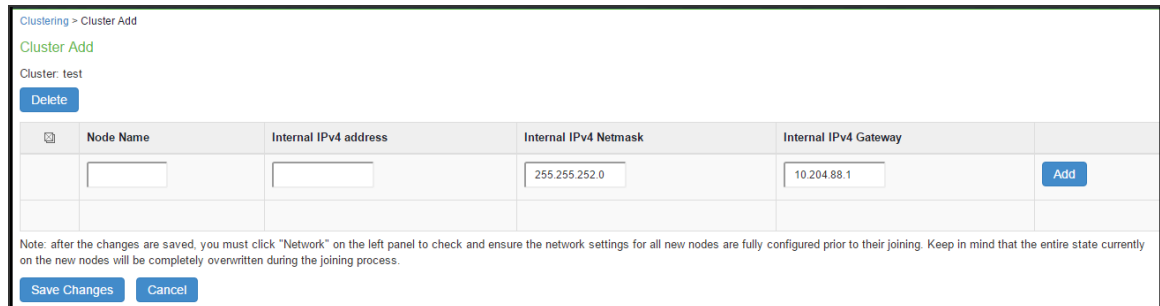
Settings	Actions
<p data-bbox="329 527 378 579"></p> <p data-bbox="418 310 1403 590">- If your cluster node configurations diverge because of changes made to one node while another is disabled or unavailable, the system manages the remerging of the configurations automatically for up to 16 updates. Beyond the maximum number of allowable updates, you might need to intervene and remerge the configurations manually. In some instances, the system might be unable to remerge the configurations if there is not enough overlapping configuration information between two nodes to manage the internode communication.</p> <p data-bbox="418 604 1393 800">- For example, for a two-node cluster in which the two nodes are partitioned from each other because of a network outage, if the internal network IP address of one of the nodes changes in one of the partitions, the two partitions are unable to rejoin, even when the network is repaired. In such a case, you must remerge the configurations manually.</p> <hr/> <p data-bbox="329 827 1393 896">If you configure your cluster as active/passive, synchronize last access time for user sessions option is automatically selected.</p>	
Network Health Check Settings	
Number of ARP Ping Failures	Specifies the number of ARP ping failures allowed before the internal interface is disabled.
Disable external interface when internal interface fails	Disables the external interface of the device if the internal interface fails.
Advanced Settings	
	Specifies the timeouts for the underlying cluster system. Do not change any values under this setting unless instructed to do so by Ivanti Global Support Center.

3. Click **Save Changes**.

Adding Cluster Members

To add multiple nodes to a cluster:

1. Select **System > Clustering > Cluster status**.
2. Click **Add Members** Enter the node name and internal IP address.
3. Modify or add the default internal netmask and internal gateway addresses, if necessary.
4. Click **Add**.



Clustering > Cluster Add

Cluster Add

Cluster: test

Delete

Node Name	Internal IPv4 address	Internal IPv4 Netmask	Internal IPv4 Gateway	
<input type="text"/>	<input type="text"/>	255.255.252.0	10.204.88.1	Add

Note: after the changes are saved, you must click "Network" on the left panel to check and ensure the network settings for all new nodes are fully configured prior to their joining. Keep in mind that the entire state currently on the new nodes will be completely overwritten during the joining process.

Save Changes Cancel

5. Repeat the process until you have added all the nodes.
6. Click Save Changes to save the node configurations.

The system automatically enables the added nodes, even if they are unreachable.

- You configure the node-specific settings for the newly added node manually because binary import options are not useful.



- The only recommended binary import option into a cluster is "Import everything except network settings and licenses" from the **Maintenance > Import/Export > Configuration** page, which restores cluster-wide configuration (sign-in, realms, roles, resource policies etc.) from a backup binary file. As this option skips node-specific settings, you must perform step 2 manually to populate the newly joined node with the right set of node-specific settings.

License Server

If a license server needs to be configured on both the nodes of a cluster, then perform the following steps:

1. Select **Configuration > Licensing > Configure Server**.
2. Select the setting for **Entire** cluster.

3. Configure the License server IP and preferred network.
4. Click **Save Changes**.

Joining a Node to an Existing Cluster

The following procedure describes how to join a node to the existing cluster.

To join additional nodes to the cluster:

1. From an existing cluster member, select the **System > Clustering > Cluster Status** tab and specify the node you want to add to the cluster.
2. Select the **System > Clustering > Join** tab and enter the following information:
 - The name of the cluster to join
 - The cluster password you specified when defining the cluster
 - The IP address of an active cluster member
3. Click **Join Cluster**. When prompted to confirm joining the cluster, click **Join**.



The join cluster operation validates IPv4 and IPv6 settings for all the physical ports (internal, external, and management) against those present in the existing cluster. For example, the external port IPv6 settings present on Node-Y are compared against external port IPv6 settings that were specified for the Node-Y add member operation entered on the primary node (Node-X). If there is a mismatch, the join operation fails with an appropriate error message.

The screenshot shows a web interface for joining an existing cluster. At the top, there is a breadcrumb 'Clustering > Join Existing Cluster' and a title 'Join Existing Cluster'. Below the title are two tabs: 'Join' (which is active and highlighted in green) and 'Create'. The form contains three input fields: 'Cluster Name' with a placeholder 'Name of the cluster to join', 'Cluster Password', and 'Existing Member Address' with a placeholder 'Internal IP address of any existing cluster member'. At the bottom of the form is a blue button labeled 'Join Cluster'.

Deleting a Cluster

If you delete a cluster, all the nodes begin running as standalone systems.

To delete a cluster:

1. Select the **System > Clustering > Properties** page.
2. Click **Delete Cluster**.
3. Click **Save Changes**.

Active/Active configuration

▼ **Synchronization Settings**

Synchronize log messages

Synchronize last access time for user sessions

▼ **Network Healthcheck Settings**

Number of ARP Ping failures before interface is disabled (should be greater than 0):

Disable external interface when internal interface fails

▼ **Advanced Settings**

Enable Advanced Settings

Verifying the Cluster Status

You can verify the cluster status on any node using System > Clustering > Cluster Status page. The list displays each node in the cluster along with its status. In an Active/Passive cluster, you can verify which node owns the VIP and you can force a manual fail over to the passive node by selecting the Fail-over VIP option.

Clustering > Cluster Status

Cluster Status

Cluster Name: test123
 Type:
 Configuration: Active/Active
 Cluster GUID: 42AB949D-11A0-774D-9FB7-6483653A24A7

10 records per page Search:

<input type="checkbox"/>	Member Name	Internal Address	External Address	Status	Notes	Sync Rank	<input type="button" value="Update"/>
<input type="checkbox"/>	* node1	10.204.54.64/20		●	Leader	<input type="text" value="0"/>	
<input type="checkbox"/>	node2	10.204.63.250/20		●	Enabled, Unreachable	<input type="text" value="0"/>	

GUI Element	Description
Status Information labels	Displays the cluster name, type, configuration, internal VIP, and external VIP for an active/passive cluster.
Add Members button	Click this button to specify a node you intend to add to the cluster. You can add multiple nodes at the same time.
Enable button	Click this button to add a node that was previously disabled. When you add a node, all state information is synchronized on the node.
Disable button	Click this button to disable a node within the cluster. The node retains awareness of the cluster but does not participate in state synchronizations or receive user requests unless members sign in to the node, directly.
Remove button	Click this button to remove the selected node or nodes from the cluster. After removal, the node runs in standalone mode.
Fail-Over VIP	Click this button to failover the VIP to the other node in the active/passive cluster. Only available if cluster is configured as active/passive.
Member Name column	Lists all nodes belonging to the cluster. You can click on a node's name to modify its name and network settings.
Internal Address column	Shows the internal IP address of the cluster member using Classless Interdomain Routing (CIDR) notation.
External Address column	Shows the external IP address of the cluster member using CIDR notation. Note that this column shows only the external IP address of the cluster leader unless you specify a different address for the node on its individual network settings page, which is accessible by clicking its name in the Member Name column. If you change the external IP address on the Network > Network Settings page, the change affects all cluster nodes.
Status column	Shows the current state of the node: Green light, Leader—The node is the active member of an active/active cluster and is handling user requests. Green light/enabled—The node is handling user requests and participating in cluster synchronization. Yellow light/transitioning—The node is joining the cluster.

GUI Element	Description
	<p>Red light/disabled—The node is not handling user requests or participating in cluster synchronization.</p> <p>Red light/enabled, unreachable —The node is enabled but because of a network issue, it cannot be reached.</p> <p>A node's state is considered standalone when it is deployed outside of a cluster or after being removed from a cluster.</p>
Notes column	<p>Shows the status of the node's connection to the cluster:</p> <p>OK—The node is actively participating in the cluster.</p> <p>ransitioning—The node is switching from the standalone state to the enabled state.</p> <p>Unreachable—The node is not aware of the cluster. A cluster member might be unreachable even when it's online and can be pinged. Possible reasons include: its password is incorrect, it doesn't have information about all cluster nodes, it's configured with a different group communication mode, it is running a different service package version, or the machine is turned off.</p>
Sync Rank column	<p>Specifies the synchronization order for nodes when a node rejoins a cluster. Accepts sync ranks from 0 (lowest rank) to 255 (highest rank). The highest rank takes precedence. If two nodes have identical sync ranks, the alphanumeric rank of the member name is used to determine precedence.</p>
Update button	<p>Updates the sync rank after you change the precedence of the nodes in the Sync Rank column.</p>

Load Balancer for Active/Active Cluster

In active/active mode, you have the option of using an external load balancer with a cluster. The load balancer hosts the cluster VIP and routes user requests to a node defined in its cluster group based on source-IP routing. If a node goes off line, the load balancer adjusts the load on the active nodes. Users do not need to sign in again.

The following are the recommendations while choosing and configuring a load balancer for your cluster:

- Listens to traffic on multiple ports
- Manages traffic using assigned source and destination IP addresses (not destination port)

To add a load balancer using an active/active configuration:

1. Select **System > Network > Load Balancer**.

Network > Load Balancer

Load Balancer

Network Settings

Overview Internal Port External Port VLANs Routes Hosts Load Balancer

Enter the load balancer settings and click the Save Changes button at the bottom of the page.

▼ Load Balancer IP Address

Enter the IP addresses used to access the internal and external interfaces of the Pulse Policy Secure.

Internal IPv4 Address:

External IPv4 Address:

Internal IPv6 Address:

External IPv6 Address:

▼ Load Balancer Usage

Use the checkboxes to specify how the load balancer is used.

Between endpoints and the Pulse Policy Secure

Between Infranet Enforcers and the Pulse Policy Secure (This option is not supported for IPv6 Addresses).

Save Changes

2. Enter the IPv4/IPv6 address of the interface connected to the load balancer in the appropriate port window. Do not enter addresses in both fields unless the load balancer is connected to both interfaces.
3. Select the appropriate load balancer usage options.
 - Between endpoints and IPS
 - Between Infranet Enforcers and IPS
4. Click **Save Changes**.

Health Checking a Server from Load Balancer

The system hosts an HTML page that provides service status for each node in a cluster. External load balancers can check this resource to determine how to effectively distribute the load among all the cluster nodes.

To perform the Layer 7 health check for a node:

Using a web browser browser, enter the URL: `https://<IPS Series device-Hostname>/dana-na/healthcheck/healthcheck.cgi?status=all`

This returns either HTTP Status 200 OK or 500 Internal Error. If this returns HTTP Status 200 OK, the following additional parameters are shown.

Parameter Name	Value	Description
CPU-UTILIZATION	0-100	Specifies the CPU utilization percentage (0-100).
SWAP-UTILIZATION	integer	Specifies the swap utilization percentage of the device (0-100).
DISK-UTILIZATION	integer	Specifies the used disk space percentage (0-100).
USER-COUNT	integer	Specifies the total number of licensed users logged in to the device. This does not include any MAC address users or Radius users.
MAX-LICENSED-USERS-REACHED	boolean	Specifies the maximum number of licensed users reached.
Platform-Limit	integer	Specifies the maximum user limit on PSA hardware.
Maximum-License-Count	integer	Specifies the maximum licenses installed directly on the PSA hardware or licenses fetched from the license server.
Cluster-Name	String	Specifies the name given to the cluster. The name must be unique across the network.

The following example performs the Layer 7 health check from an external load balancer:

```
GET /dana-na/healthcheck/healthcheck.cgi?status=all HTTP/1.1\r\nHost: localhost\r\n\r\n
```

The concept of receive string is used for health check. The receive string is configured on the load balancer is used to decide whether the node is active or inactive. It is a regular expression that checks for a value present in the response. For example, IPS sends a page to the load balancer that has USER-COUNT=25 indicating that the number of active licensed users on that device is 25.

A receive string of `USER-COUNT\=[([0-9])([0-9][1-9])100]`; means check if USER-COUNT is between 0 and 100. In this example, 25 is between 0 and 100 and the load balancer marks the device as active and considers it for load balancing.

Health check details:

```
CPU-UTILIZATION=4;  
SWAP-UTILIZATION=0;  
DISK-UTILIZATION=6;  
SSL-CONNECTION-COUNT=4;  
PLATFORM-LIMIT=500;  
MAXIMUM-LICENSED-USER-COUNT=200;  
USER-COUNT=1;  
MAX-LICENSED-USERS-REACHED=NO;  
CLUSTER-NAME=IFMAP;
```

Serial Console Configuration

If you are adding a factory-set device to a cluster, we recommend that you use the serial console, which enables you to join an existing cluster during the initialization process by entering minimal information. When a node joins a cluster, it receives the cluster state settings, which overwrite all settings on a device with an existing configuration and provide new machines with the required preliminary information. You can also use the serial console to disable the node. If the node is in a synchronization state, you cannot access its admin console. Therefore, if you need to upgrade or reboot the node, for example, you must first disable the node from a cluster through its serial console.

Joining a Node to a Cluster

To add a node to a cluster through its serial console:

1. Connect to the serial console of the device you want to add to the cluster.
2. Reboot the device and watch its serial console. After the system software starts, a message appears stating that the device is about to boot as a standalone node and to press the Tab key for clustering options. Press the Tab key as soon as you see this option.



The interval to press the Tab key is five seconds. If the device begins to boot in standalone mode, wait for it to finish and then reboot again.

3. Enter 2 to join an existing cluster.

4. Enter the requested information, including:
 - The internal IP address of an active member in the cluster
 - The cluster password, which is the password you entered when defining the cluster
 - The name of the device to add
 - The internal IP address of the device to add
 - The netmask of the device to add
 - The gateway of the device to add
5. The active cluster member verifies the cluster password and that the new device's name and IP address match what you specified in the admin console. If the credentials are valid, the active member copies all its state data to the new cluster member, including certificate, user, and system data.

From the Admin Console, select System > Clustering > Cluster Status of any active cluster member to confirm that the new member's Status is green, indicating that the node is now an enabled node of the cluster (status is green).



If you add a node running an earlier version service package to a cluster, the node automatically detects the mismatch, gets the newer package from the cluster, and joins the cluster.

Disabling a Clustered Node

To disable a node within a cluster using its serial console:

1. Connect to the serial console of the device you want to disable within the cluster
2. Enter 4 for the System Operations option.
3. Enter 8 for Disable Node option.
4. Enter y when the serial console prompts you to confirm that you want to disable the node.
5. From the Admin console, verify that the node has been disabled (status is red) within the cluster by selecting **System > Clustering > Status** of any active cluster member.

Restarting or Rebooting Cluster Nodes Using Its Serial Console

When you create a cluster of two or more nodes, the clustered nodes act as a logical entity. When you reboot one of the nodes using either the serial console or the admin console, all nodes in the cluster restart or reboot.

To reboot only one node:

1. Connect to the serial console of the device you want to disable within the cluster.
2. Enter 4 for System Operations option.
3. Select **System > Clustering > Status** to disable the node you want to restart or reboot within the cluster.
4. Under system operations select the appropriate menu option 9 <Reboot this device>, 10 <Shutdown this device>, or 11 <Restart Services>.
5. Reboot the node, then enable the node within the cluster again.

WAN Clustering

Overview

A WAN cluster is a group of independent servers/nodes separated by WAN networks working together as a single system to provide load balancing and high scalability for clients and services. WAN cluster works only in active-active cluster operation mode and is qualified on PSA7000, PSA7000-V, PSA5000, PSA5000-V and PSA3000 platforms.

Clustering supports following types of synchronization settings:

- Configuration-only Cluster - Only configuration will be synced across the cluster nodes
- Synchronize user sessions - Configuration and user session information will be synced across the Cluster nodes



WAN cluster only supports Configuration-only Cluster and does not support Synchronize user sessions.

Configuring an Active-Active Configuration-only WAN Cluster

To configure an Active/Active Configuration-only WAN cluster:

1. Configure an Active/Active cluster as mentioned in the "[Configuring an Active/Active or Active/Passive Cluster](#)" on page 940 section.
2. Select **System > Clustering > Cluster Properties** and select **Configuration-only Cluster** as shown in the screen below.

The screenshot shows the 'Cluster Properties' configuration page. The 'Type' is set to 'PSA-5000' and the 'Cluster Name' is 'wan_cluster'. Under 'Configuration Settings', 'Active/Active configuration' is selected. Under 'User/Session Synchronization', the 'Configuration-only Cluster' option is selected and highlighted with a red box. A warning message is visible below: 'WARNING: Enabling the "Configuration-only Cluster" feature limits data transfers between the cluster nodes. User and Session specific limits are only enforced on the node and not across the cluster. Please be aware of the limitations of this deployment.' Other options include 'Synchronize log messages' and 'Synchronize user sessions'.

3. Under **Advanced Settings**, select **Enable Advanced Settings** and then select the **Network Type as Average latency 60-100ms** or **Average latency 10-60ms** for WAN cluster.

The screenshot shows the 'Cluster Properties' configuration page with 'Advanced Settings' expanded. 'Enable Advanced Settings' is checked. Under 'Network Type', the 'Network type selection' dropdown is open, showing options: 'Default', 'Average latency 10-100ms', 'Average latency 1-10ms', and 'Average latency 60-100ms'. The 'Average latency 60-100ms' option is selected. A warning message is visible: 'WARNING: Changing the network type will result in cluster services being restarted. The underlying cluster system. Change this value only when you observe repeated cluster partitions that may be related to long network delays or significant load in any of the cluster nodes with non default timeout multipliers (see below). If a non default network type is picked, the timeout multiplier will silently get reset to the default value.' At the bottom, there are 'Save Changes' and 'Delete Cluster...' buttons.



In an Active/Active WAN cluster, if the networks of all the internal ports of the IPS/Nodes are in different subnets, it is mandatory to add specific static network routes on every IPS/Node to reach every other IPS/Node in the cluster for better cluster communication during IPS/Node failover or downtime.

To add a specific static route on a IPS/Node to reach another IPS/Node in the cluster:

1. Select **System > Network > Routes**.
2. Click **New Route**.

Network Settings (for node cluster_1) Routes

View route table for: Internal IPv4 Update

Many networks will not require changes to these routing tables, but if you need to add additional routes, you can do so here.

New Route... Delete...

Internal Port	Status	Destination Network/IP	Netmask	Gateway	Interface	Metric (0-15)
default	●	10.11.0.0	255.255.0.0	0.0.0.0	Internal	0
default	●	0.0.0.0	0.0.0.0	10.11.1.1	Internal	0

3. Based on the Network's Topology the Static Route needs to be added on IPS/Node to reach other IPS/Node in WAN Cluster. Below is an example where static route is added on IPS Configured in 10.11.0.0/16 network having gateway 10.11.1.1 to reach another IPS/Node Configured in 10.12.0.0/16.

Network Settings (for node cluster_1) Internal Port - New Route

Network Settings (for node cluster_1) > Routes > New Route

Destination Network/IP: 10.12.0.0

Netmask: 255.255.0.0

Gateway: 10.11.1.1

Interface: Internal

Metric:

Add to Internal route table Cancel

4. The same steps need to be repeated on every IPS/Node in the Active/Active WAN cluster.

Monitoring and Troubleshooting

If you have a problem with a cluster, a representative from Ivanti Global Support Center might ask you to create a snapshot that includes group communication statistics to assist with debugging the cluster problem. When you enable the group communication monitor, the system records statistics related to all the cluster nodes. As the local node communicates with other nodes in the cluster, the system captures statistics related to intra cluster communication. The Group Communication tab is displayed only when you enable clustering on your system. On a standalone system, you do not have access to the Group Communication tab.

You can also enable the cluster networking troubleshooting server on the Network Connectivity page.



- Performing excessive node monitoring can impact system performance and stability. You should only perform extensive monitoring when directed by your Ivanti Global Support Center representative.
 - Performing log synchronization across cluster nodes can impact your system performance and stability.
-

Group Monitoring

To enable group communication monitoring:

- Enter the maximum size of the statistics log.
- Enter the interval, in seconds, at which events are to be logged.

If you want to monitor all cluster nodes from the current local node, select the **Monitor all cluster nodes** from this node check box. If you do not check this option, the group communication monitor gathers statistics only for the local node.



If you select the Monitor all cluster nodes from this node option, the cluster nodes must be able to communicate over UDP port 6543

1. Select the **Enable group communication monitoring** check box to start the monitoring tool.
2. Click **Save Changes**.

The screenshot shows a web interface for configuring Group Communication monitoring. The breadcrumb trail is "Troubleshooting > Monitoring > Cluster > Group Communication". The page title is "Group Communication". There are tabs for "User Sessions", "Monitoring" (which is active), "Tools", "System Snapshot", and "Remote Debugging". Below these are sub-tabs for "Debug Log", "Node Monitor", "Cluster" (which is active), and "Diagnostic Logs". The main content area has a sub-tab for "Group Communication" and "Network Connectivity". A message states: "This page allows you to start and stop the group communication monitoring and statistics gathering tool at the local node." Below this, it says "Monitoring is OFF". There are two input fields: "Maximum statistics log size" with a value of "1" and unit "MBytes" (range 1-5), and "Monitoring interval" with a value of "10" and unit "Seconds" (range 5-60). There are two checkboxes: "Monitor all cluster nodes from this node" (unchecked) and "Enable group communication monitor" (unchecked). A note next to the second checkbox says: "For this option to work correctly, cluster nodes must be able to communicate over UDP port 6543." At the bottom left is a "Save Changes" button.

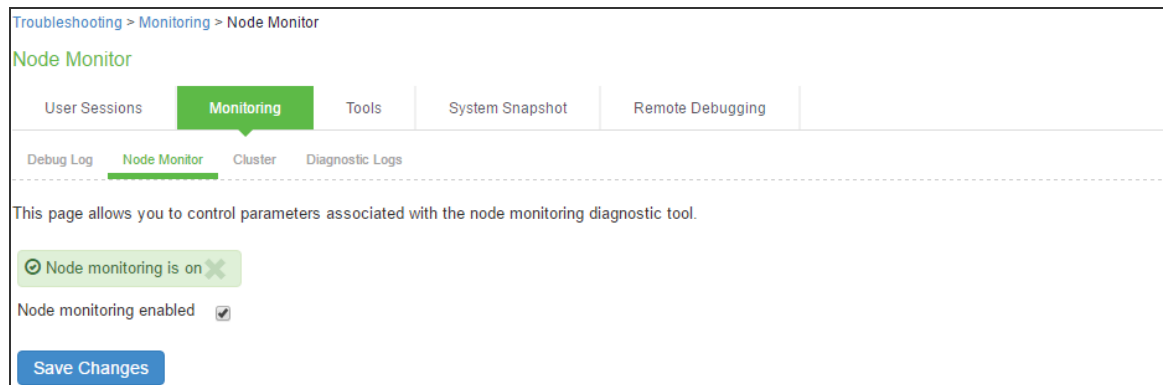
3. If you want to include the node monitoring results in the system snapshot, choose **Maintenance > Troubleshooting > System Snapshot**, and select the Include debug log check box.
4. Take a system snapshot to retrieve the results.

Node Monitoring

To enable node monitoring:

1. Select **Maintenance > Troubleshooting > Monitoring > Node Monitor** to enable the node monitor.
2. Enter the maximum size for the node monitor log.
3. Enter the interval, (in seconds) at which node statistics are to be captured.

4. Select the Node monitoring enabled check box to start monitoring cluster nodes.



5. For Maximum node monitor log size, enter the maximum size (in MB) of the log file. Valid values in the range of 1 - 30.
6. Specify the interval (in seconds) that defines how often nodes are to be monitored.
7. Select the commands to use to monitor the node.
8. If you select dsstatdump, enter its parameters as well.
9. Click **Save Changes**.
10. To include the node monitoring results in the system snapshot, select Maintenance > Troubleshooting > System Snapshot, and select the Include debug log check box.
11. Take a system snapshot to retrieve the results.

Network Connectivity Monitoring

Use the Network Connectivity tab to enable the cluster node troubleshooting server and to select a node on which to perform troubleshooting tasks. The troubleshooting tool allows you to determine the network connectivity between cluster nodes.

The server component of this tool runs on the node to which connectivity is being tested. The client component runs on the node from which connectivity is being tested. The basic scenario for testing connectivity is this:

- The administrator starts the server component on the passive node.
- The administrator tests the connectivity to the server node from the Active node, by starting the client component on the active node and then contacting the passive node running the server component.



The server component must be run on nodes that are configured as either standalone or in a cluster but disabled. Cluster services cannot be running on the same node as the server component.

To enable network connectivity monitoring:

1. Select **Maintenance > Troubleshooting > Cluster > Network Connectivity** and **Enable cluster network troubleshooting server** check box to enable the server component.

The screenshot shows the 'Network Connectivity' configuration page. The breadcrumb trail is 'Troubleshooting > Monitoring > Cluster > Network Connectivity'. The page has several tabs: 'User Sessions', 'Monitoring' (selected), 'Tools', 'System Snapshot', and 'Remote Debugging'. Below the tabs, there are sub-sections for 'Debug Log', 'Node Monitor', 'Cluster' (selected), and 'Diagnostic Logs'. Under 'Cluster', there are sub-sections for 'Group Communication' and 'Network Connectivity' (selected). A descriptive paragraph explains that this page provides a means of testing network connectivity between nodes in a cluster. The 'Troubleshooting Server' section has a checked checkbox for 'Enable cluster network troubleshooting server' and a 'Client Node' input field. The 'Troubleshoot Node' section has a 'Select Node' dropdown menu set to 'Standalone Device' and a 'Go' button. There are also 'Save Changes' and 'Go' buttons.

2. Click **Save Changes**.
3. On another machine, select **Maintenance > Troubleshooting > Cluster > Network Connectivity**.

Perform one of the following steps:

- Select a node from the list.
 - Enter the IP address of the server node.
4. Click Go to begin troubleshooting the machine on which the server component is running.
 5. Click the Details link below the fields to view the results.

Monitoring using SNMP Traps

You can monitor clusters using the standard logging tools. Specifically, you can use several cluster-specific SNMP traps to monitor events that occur on your cluster nodes, such as:

- External interface down
- Internal interface down
- Disabled node
- Changed virtual IP address (VIP)
- Deleted cluster node (cluster stop)



In general, it is desirable to configure your SNMP traps on a clusterwide basis so that any given cluster node can send its generated traps to the right target. Setting up clusterwide configuration for the traps is particularly important when you also use a load balancer, because you might not know which node is responsible for a specific operation. In that case, the load balancer can independently determine which cluster node can manage an administrative session.

You can use SNMP traps that are included in the Ivanti Standard MIB to monitor these events. These traps include:

- `iveNetExternalInterfaceDownTrap`—Supplies type of event that brought down the external interface.
- `iveNetInternalInterfaceDownTrap`—Supplies type of event that brought down the internal interface.
- `iveClusterDisableNodeTrap`—Supplies the cluster name on which nodes are disabled, along with a space-separated list of disabled node names.
- `iveClusterChangedVIPTrap`—Supplies the type of the VIP, whether external or internal, and its value before and after the change.
- `iveClusterDelete`—Supplies the name of the cluster node on which the cluster delete event was initiated.

These traps are always enabled and available in the MIB. You cannot disable the traps.

Troubleshooting

You can use a built-in feature on the clustering Status page to identify the status of each cluster node. Mouse over the Status light icon to display a tool tip containing a hexadecimal number. The hexadecimal number is a snapshot of the status of the system.

Value	Meaning
0x000001	System is in standalone mode.
0x000002	System is in cluster disabled state.
0x000004	System is in cluster enabled state.
0x000008	System is unreachable (because it is offline, has the wrong password, has a different cluster definition, different version, or other problem).
0x0002000	The node owns the VIPs (on) or not (off).
0x000100	System is synchronizing its state from another node (initial synchronizing phase).
0x000200	System is transitioning from one state to another.
0x00020000	Group communication subsystems at the local and remote nodes are disconnected from each other.
0x00040000	Management interface (mgt0) is displayed disconnected.
0x00080000	Management gateway is unreachable for ARP ping.
0x000800	Interface int0 displays disconnected (no carrier).
0x001000	Interface int1 displays disconnected (no carrier).
0x002000	System is syncing its state to another node that is joining.
0x004000	Initial Synchronization as master or slave is taking place.
0x008000	System is the leader of the cluster.
0x010000	The spread daemon is running and the cache server is connected to it.
0x020000	The gateway on int0 is unreachable for ARP pings (see log file).
0x040000	The gateway on int1 is unreachable for ARP pings (see log file).
0x080000	Leader election is taking place.

Value	Meaning
0x100000	Server lifecycle process is busy.
0x200000	System is performing post state synchronization activities.
0x30004	The spread daemon is running and the cache server is connected to it. The gateway on int0 is unreachable for ARP pings (see log file). System is in cluster enabled state.
0x38004	The spread daemon is running and the cache server is connected to it. The gateway on int0 is unreachable for ARP pings (see log file). System is the leader of the cluster. System is in cluster enabled state.

Each code, as you see it in the system, may relate specifically to one state. However, each code may represent a combination of states, and so the actual code does not appear in the above table. Instead, the code you see in the system is the sum of several of the hexadecimal numbers shown above. You will need to factor out the codes, as in the following example:

- 0x38004—The rightmost digit (4) in this hexadecimal number corresponds to:
 - 0x000004—The system is in a cluster enabled state.
- 0x38004—The digit in the fourth position from the right (8) corresponds to:
 - 0x008000—This system is the leader of the cluster.
- 0x38004—The leftmost digit (3) in this hexadecimal number does not exist in the table, which indicates that it corresponds to the sum of two other digits, in this case, 1 and 2, as shown in the following codes:
 - 0x020000—The gateway on int0 is unreachable for ARP pings (see log file).
 - 0x010000—The spread daemon is running and the cache server is connected to it.

Restarting or Rebooting Cluster Nodes

When you create a cluster of two or more nodes, the clustered nodes act as a logical entity. When you reboot one of the nodes using either the serial console or the admin console, all nodes in the cluster restart or reboot.

To reboot only one node:

1. Select **System > Clustering > Status** to disable the node you want to restart or reboot within the cluster.
2. Select **Maintenance > System > Platform**.
3. Reboot the node, then enable the node within the cluster again.

Appendix

Licensing

Ivanti Policy Secure(IPS) software includes Ivanti Licensing and Software Download Center @ <https://my.pulsesecure.net>, that lets you configure the license server to allow administrators to view all configured systems and move those licenses as needed. Other devices on the network lease licenses from the central license server. For more information, see *License Management Guide*.

Starting with IPS version 5.0, clustering works as follows:

- Clustering does not require a license.
- Place an equal number of licenses on each appliance, when they are joined together to form a cluster, the user licenses add up so that the cluster supports all the licensed users.
- For example, building a 1,000-user cluster is done by bringing together two appliances with 500 user licenses in each of the two units.
- For third-party features, each node in a cluster should have similar license counts.
- The maximum number of concurrent users allowed in a cluster is the sum of all user licenses of all connected nodes.

If your client devices are using IPS prior to release 5.0:

- A license is no longer required to create a cluster. Prior to Release 4.0, to create a multiple node cluster that supports multiple concurrent users, you were required to purchase one ADD-ccccE license for one cluster node, and n-1 CL licenses (one for each of the remaining cluster nodes). For example, to create a 4-node cluster supporting 2000 concurrent users, you needed to purchase one ADD-2000E license and 3 CL licenses.

- CL licenses are no longer necessary but are still supported. When you upgrade to Release 4.0, your existing licenses continue to work. There is no cluster grace period for the node with a CL license installed. When the node with a CL license installed disconnects, the capacity computation is the same as before Release 4.0.
- A 5-day cluster grace period provides license flexibility when a node crashes or loses connectivity with the rest of the cluster.
- We recommend that you distribute your ADD licenses equally across the cluster to avoid losing large number of licenses when a node disconnects from the cluster.

The following table illustrates why we recommend distributing licenses equally across all cluster nodes.

License Distribution	Example
Example 1: Equal distribution	<p>Suppose Node A and Node B are part of a cluster, and each node has 500 concurrent user licenses then the maximum number of licenses is 1000. Suppose Node B disconnects from the cluster. Until the clustering grace period ends, the maximum number of licenses on Node A is 500 (from Node A's original license) + minimum (licenses on Node A (500), licenses on Node B (500)) = 500 + 500 = 1000. After the grace period ends, the maximum number of licenses on Node A reverts to its original license of 500.</p>
Example 2: Unequal distribution	<p>In this example, Node A and Node B are part of a cluster. Node A has 600 ADD licenses and Node B has 400 ADD licenses then the maximum number of licenses is 1000. Suppose Node B disconnects from the cluster. Until the clustering grace period ends, the maximum number of licenses on Node A is 600 (from Node A's original license) + minimum (licenses on Node A (600), licenses on Node B (400)) = 600 + 400 = 1000. After the grace period ends, the maximum number of licenses on Node A is 600. Suppose Node A disconnects from the cluster. Until the clustering grace period ends, the maximum number of licenses on Node B is 400 (from Node B's original license) + minimum (licenses on Node A (600), licenses on Node B (400)) = 400 + 400 = 800. After the grace period ends, the maximum number of licenses on Node B is 400.</p>

License Distribution	Example
<p>Example 3. Unequal distribution (extreme)</p>	<p>In this example, Node A and Node B are part of a cluster. Node A has 1000 ADD licenses and Node B has no ADD licenses.</p> <p>Suppose Node B disconnects from the cluster. Until the clustering grace period ends, the maximum number of licenses on Node A is 1000 (from Node A's original license) + minimum (licenses on Node A (1000), licenses on Node B (0)) = 1000 + 0 = 1000. After the grace period ends, the maximum number of licenses on Node A is 1000.</p> <p>Suppose Node A disconnects from the cluster. Until the clustering grace period ends, the maximum number of licenses on Node B is 0 (from Node B's original license) + minimum (licenses on Node A (1000), licenses on Node B (0)) = 0 + 0 = 0. After the grace period ends, the maximum number of licenses on Node B is 0.</p> <p>For the scenarios in Examples 2 and 3, we recommend you distribute the licenses equally amongst the nodes.</p>

Configuring IPv6 on an Existing IPv4 Active/Passive Cluster

We recommend as a best practice that you configure IPv6 host and network settings on individual nodes before you create a cluster. In some cases, such as routine upgrade, you have already created a cluster configuration and only want to add IPv6 addresses to the existing interface configuration. If so, follow the procedures in this section precisely.



You must leave IPv6 disabled until the last step of the procedures shown below.

To modify the internal port configuration for the cluster:

1. Select **System > Network > Internal Port > Settings**.
2. Under **Settings for**, select **Entire cluster**.
3. Complete the configuration for the IPv6 prefix and the IPv6 gateway, but do not enable IPv6.
4. Verify that all the nodes are up and running, are in sync, and are in reachable state. Complete synchronization of the cluster pair might take a few minutes.
5. Under **Settings for**, select **Node 1**.

6. Configure the IPv6 address, but do not enable IPv6.
7. Verify both the nodes are up and running and in reachable state.
8. Repeat steps 6-8 for **Node 2**.
9. Select **System > Network > Internal Port > Virtual Ports**.
10. Update the cluster virtual port configuration to add the IPv6 address.
11. Select **System > Network > Internal Port > Settings**.
12. Under **Settings for**, select **Entire cluster**.
13. Select **Enable IPv6**.

To modify the external port configuration for the cluster:

1. Select **System > Network > External Port > Settings**.
2. Under **Settings for**, select **Entire cluster**.
3. Complete the configuration for the IPv6 prefix and the IPv6 gateway, but do not enable IPv6.
4. Verify that all the nodes are up and running, are in sync, and are in reachable state. Complete synchronization of the cluster pair might take a few minutes.
5. Under **Settings for**, select **Node 1**.
6. Configure the IPv6 address, but do not enable IPv6.
7. Verify both the nodes are up and running and in reachable state.
8. Repeat steps 6-8 for Node 2.
9. Select **System > Network > External Port > Virtual Ports**.
10. Update the cluster virtual port configuration to add the IPv6 address.
11. Select **System > Network > External Port > Settings**.
12. Under **Settings for**, select **Entire cluster**.
13. Select **Enable IPv6**.

Cloud Secure

Cloud Secure provides secure, seamless, and compliant access to cloud resources on a hybrid IT environment where companies are combining the best of the cloud with their own localized data centers. Cloud Secure solution integrates with multiple Ivanti products such as Ivanti Connect Secure, Ivanti Policy Secure, Pulse Workspace etc.

Cloud Secure provides great level of flexibility with integration to various Third-Party vendors such as MDM vendors, IdP vendors etc. It is a licensed feature, so the Administrator should procure and install the required license.

For more details about the configuration, various deployment scenarios, reports, etc. refer to Cloud Secure documentation available on <https://www.ivanti.com/support/product-documentation>.

For On-Premise deployment usecase, see Configuring IPS for On-Premise users.

For Cloud Application Visibility, see CAV Overview.

System Management

System management includes the following:

- [Network and Host Administration](#)
- [FIPS Level 1 Support](#)
- [Certificate Security Administration](#)
- [File Management](#)
- [Dashboard and Reports](#)
- [System Maintenance](#)

Network and Host Administration

Network and Host Administration Overview

When you install and initially set up the device, you use the serial port console to set basic network and host settings. To get started, you must use the serial console to configure these settings for the internal interface. You have the option to use the serial console to configure network and host settings for the external interface and the management interface. The network and host settings you configure with the serial port console include:

- IPv4/IPv6 address
- Netmask
- Default gateway
- Speed and duplex
- MTU
- DNS
- Default domain
- WINS

Once the internal interface has been configured, you can use the admin console Network Settings pages to modify settings for the internal interface, to enable and configure the external interface and the management interface, and to configure or manage advanced networking features, including:

- Hostname
- IPv6 addresses
- VLAN ports
- Virtual ports
- Route table entries
- Host mapping table entries
- ARP cache entries

- Neighbor discovery cache entries
- System date and time (manual configuration) or NTP

Configuring the Internal Port

The internal port connects to the local area network (LAN). The internal port settings are configured when you run the setup wizard from the serial console as part of the installation procedure. You can use the System > Network pages to make changes to the configuration.

To modify the internal port configuration:

1. Select **System > Network > Internal Port > Settings** to display the configuration page.
2. Complete the configuration as described in table.
3. Save your changes.

Settings	Guidelines
IPv4 Settings	
IP Address	Assign an IP address. You must assign an IPv4 address to the internal interface.

Settings	Guidelines
	<p>An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.</p> <p>The format of an IPv4 address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0 to 255.</p>
Netmask	<p>Assign a netmask. A netmask indicates which part of an IP address indicates network identification and which part indicates the host identification. For example, the IP address and netmask 10.20.30.1 255.255.255.0 (or 10.20.30.1/24) refer to all the hosts in the 10.20.30.0 subnet. The IP address and netmask 10.20.30.1 255.255.255.255 (or 10.20.30.1/32) refer to a single host.</p>
Default Gateway	<p>Specify the IPv4 address for the default gateway for the routing domain to which the device belongs.</p> <p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p>
IPv6 Settings	
Enable IPv6 / Disable IPv6	<p>Disabled by default. Enable to support access from IPv6 endpoints.</p> <p>When you enable IPv6, the system acquires a link local address.</p> <p>If you switch from enabled to disabled, the system clears the link local address.</p>
Link Local Address	<p>Display the auto configured link local address (after you have enabled and saved the IPv6 configuration).</p>
IPv6 Address	<p>Specify a routable IPv6 address, such as a global unicast address that your network plan has provisioned for this host and interface. Automatic configuration methods are not supported. You must specify the appropriate address manually.</p>
Prefix Length	<p>Specify how many of the higher order contiguous bits of the IPv6 address comprise the prefix (the network portion of the IPv6 address). The default is 64.</p>
Gateway	<p>Specify the IPv6 address for the default gateway for the routing domain to which the device belongs.</p> <p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p>
Advanced Settings	

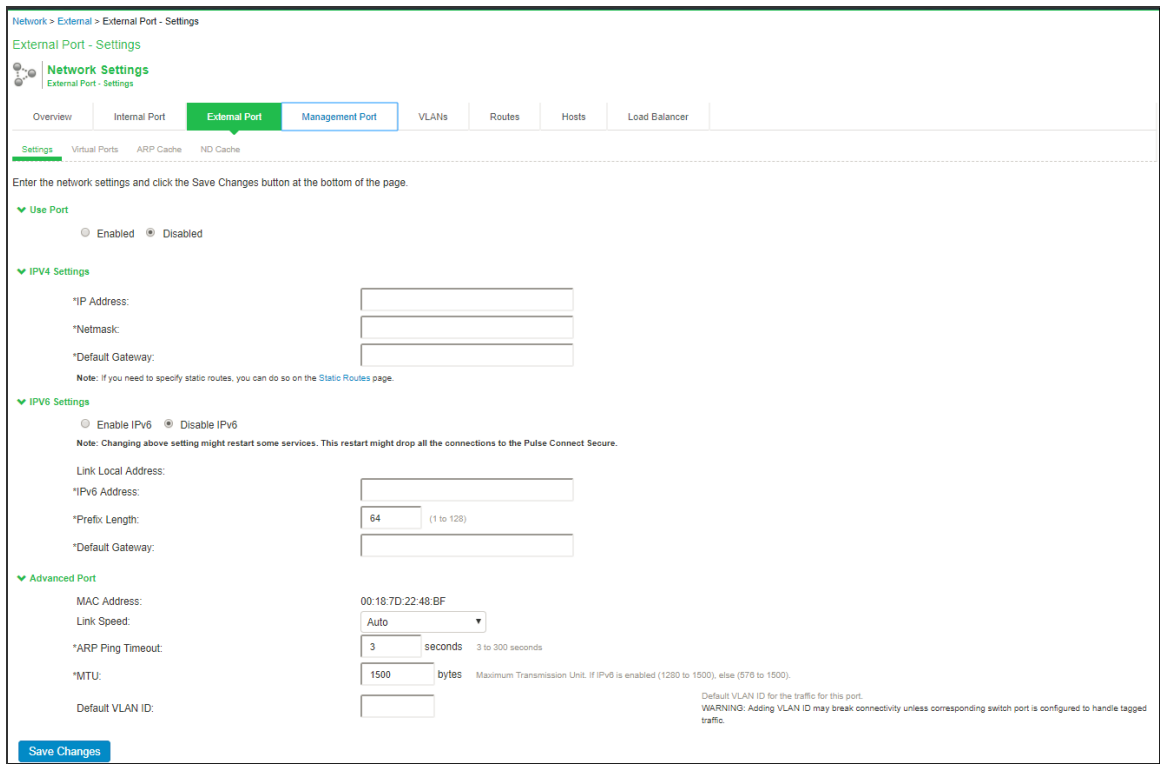
Settings	Guidelines
MAC Address	Display the MAC address for the interface.
Link Speed	Specify the speed and duplex combination for the interface. If you run SNMP_GET and then change the Link Speed value, you must wait at least 5 minutes after submitting the change before running SNMP_GET again.
ARP Ping Timeout	(IPv4 only) Specify how long the system should wait for responses to Address Resolution Protocol (ARP) requests before timing out. Cluster nodes send ARP requests to the gateways of other nodes to determine if they are properly communicating with one another. If you have not deployed a cluster, the system does not use this setting. If the node belongs to a cluster, the timeout interval that you specify is synchronized across the cluster. In multisite clusters, you can override this setting for the individual nodes in the cluster using options in the System > Clustering page. Use caution when changing this setting in active/passive clusters, however, because the system also uses the ARP Ping Timeout setting on the Internal tab as a failover timer for the VIP.
MTU	Specify the maximum transmission unit. If IPv6 is enabled, the valid range is 1280 to 1500. If IPv6 is not enabled, the valid range is 576 to 1500. We recommend you retain the default MTU setting (1500) unless you must change the setting for troubleshooting purposes.
Default VLAN ID	(Optional) Specify the default VLAN ID for the traffic of this port. When this parameter is set, all the traffic on this interface is subsequently tagged with the set VLAN ID and also accepts only incoming traffic with the same tag. Necessary changes are required on the connected switch port to handle bi-directional tagged traffic. <hr/> <ul style="list-style-type: none">- If default VLAN ID is set incorrectly or the connected switch port is not configured accordingly, the interface can become unreachable.- Default VLAN ID cannot be set if IPv6 is enabled.- Default VLAN ID is supported in a clustered environment.- In case of VMware ESXi based Virtual Appliance(VA), set the vSwitch configuration to port 4095 to allow IPS to tag the traffic.- The set default VLAN ID should be added as a member in the physical port of switch and the same VLAN should be removed from native VLAN ID. <hr/>

Configuring the External Port

The external port connects to the Internet. You can use the System > Network pages to configure the external port.

To configure the external port:

1. Select **System > Network > External Port > Settings** to display the configuration page.
2. Complete the configuration as described in table.
3. Save your changes.



Settings	Guidelines
Use Port?	
Use Port?	Select Enabled to use the port; otherwise, select Disabled.
IPv4 Settings	

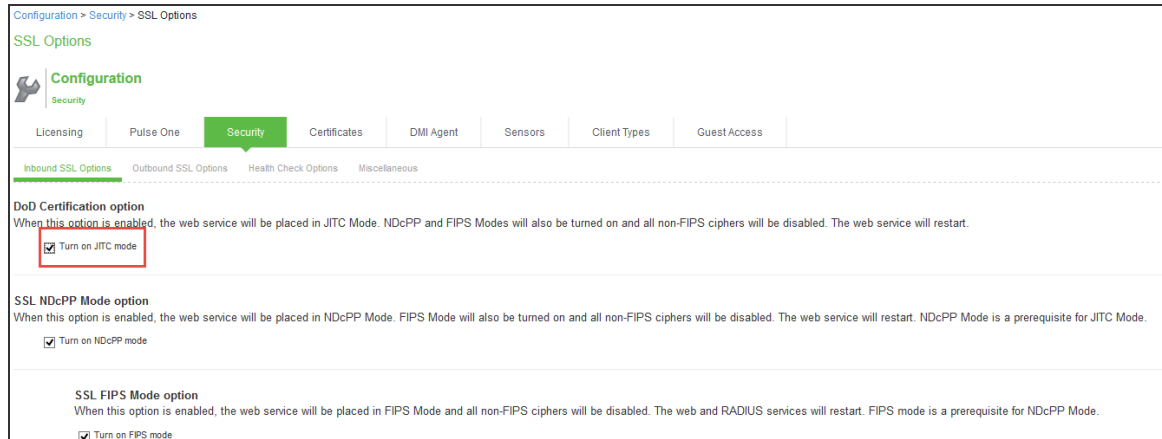
Settings	Guidelines
IP Address	<p>Specify an IP address. An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.</p> <p>The format of an IPv4 address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0 to 255.</p>
Netmask	<p>Specify a netmask. A netmask indicates which part of an IP address indicates network identification and which part indicates the host identification. For example, the IP address and netmask 10.20.30.1 255.255.255.0 (or 10.20.30.1/24) refer to all the hosts in the 10.20.30.0 subnet. The IP address and netmask 10.20.30.1 255.255.255.255 (or 10.20.30.1/32) refer to a single host.</p>
Default Gateway	<p>Specify the IPv4 address for the default gateway for the routing domain to which the device belongs.</p> <p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p>
IPv6 Settings	
Enable IPv6 / Disable IPv6	<p>Disabled by default. Enable to support access from IPv6 endpoints.</p> <p>When you enable IPv6, the system acquires a link local address.</p> <p>If you switch from enabled to disabled, the system clears the link local address.</p>
Link Local Address	<p>Display the auto configured link local address (after you have enabled and saved the IPv6 configuration).</p>
IPv6 Address	<p>Specify a routable IPv6 address, such as a global unicast address that your network plan has provisioned for this host and interface. Automatic configuration methods are not supported. You must specify the appropriate address manually.</p>
Prefix Length	<p>Specify how many of the higher order contiguous bits of the IPv6 address comprise the prefix (the network portion of the IPv6 address). The default is 64.</p>
Gateway	<p>Specify the IPv6 address for the default gateway for the routing domain to which the device belongs.</p> <p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p>
Advanced Settings	

Settings	Guidelines
MAC Address	Display the MAC address for the interface.
Link Speed	Specify the speed and duplex combination for the interface. If you run SNMP_GET and then change the Link Speed value, you must wait at least 5 minutes after submitting the change before running SNMP_GET again.
ARP Ping Timeout	(IPv4 only.) Specify how long the system should wait for responses to Address Resolution Protocol (ARP) requests before timing out. Cluster nodes send ARP requests to the gateways of other nodes to determine if they are properly communicating with one another. If you have not deployed a cluster, the system does not use this setting. If the node belongs to a cluster, the timeout interval that you specify is synchronized across the cluster. In multisite clusters, you can override this setting for the individual nodes in the cluster using options in the System > Clustering page. Use caution when changing this setting in active/passive clusters, however, because the system also uses the ARP Ping Timeout setting on the Internal tab as a failover timer for the VIP.
MTU	Specify the maximum transmission unit. If IPv6 is enabled, the valid range is 1280 to 1500. If IPv6 is not enabled, the valid range is 576 to 1500. We recommend you retain the default MTU setting (1500) unless you must change the setting for troubleshooting purposes.
Default VLAN ID	(Optional) Specify the default VLAN ID for the traffic of this port. When this parameter is set, all the traffic on this interface is subsequently tagged with the set VLAN ID and also accepts only incoming traffic with the same tag. Necessary changes are required on the connected switch port to handle bi-directional tagged traffic. <hr/> <ul style="list-style-type: none">- If default VLAN ID is set incorrectly or the connected switch port is not configured accordingly, the interface can become unreachable.- Default VLAN ID cannot be set if IPv6 is enabled.- Default VLAN ID is not supported in a clustered environment.- In case of VMware ESXi based Virtual Appliance(VA), set the vSwitch configuration to port 4095 to allow IPS to tag the traffic.- The set default VLAN ID should be added as a member in the physical port of switch and the same VLAN should be removed from native VLAN ID. <hr/>

JITC Mode Option

To enable the Joint Interoperability Test Command (JITC) mode:

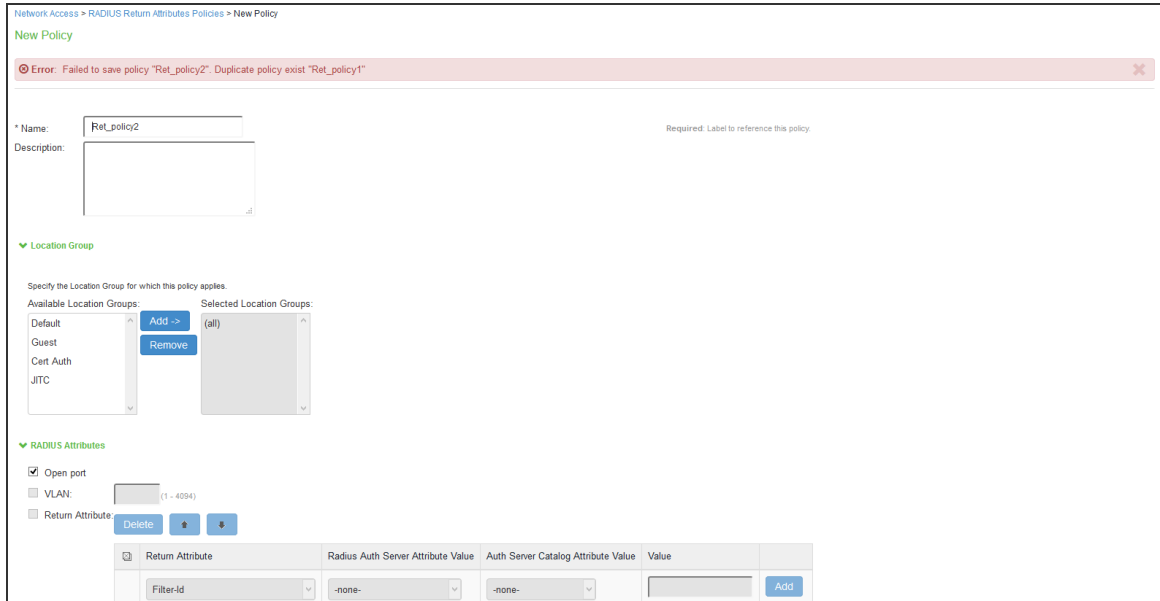
1. Select **System > Configuration > Security > Inbound SSL Options**.
2. Under **DoD certification** option, enable **Turn on JITC mode**.



NDcPP and FIPS mode are automatically enabled after enabling the **JITC mode**.

3. Click **Save Changes**.

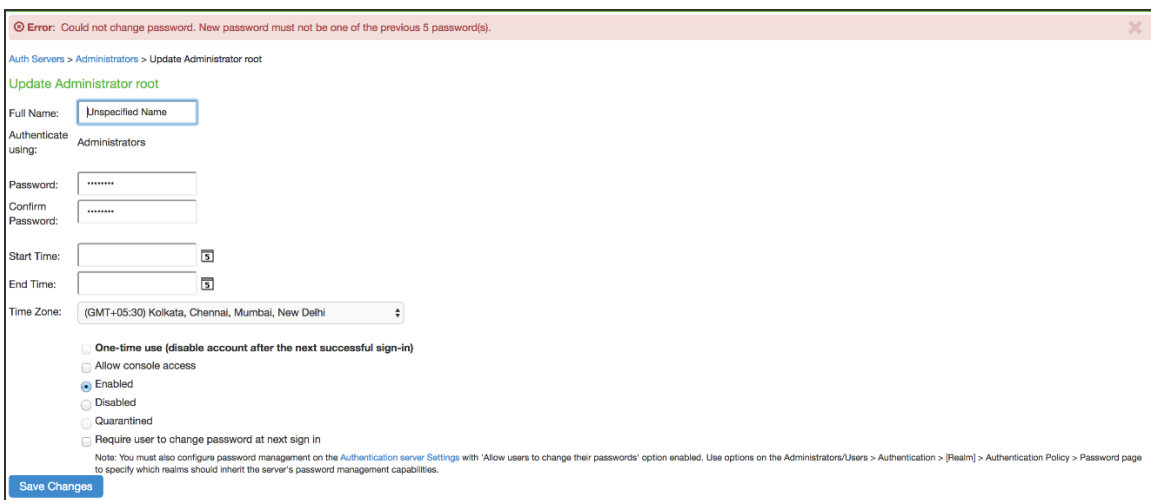
- With JITC mode enabled, IPS detects any duplicate RADIUS Return and Request Attribute policies and an error message is displayed if the user tries to create a duplicate policy.



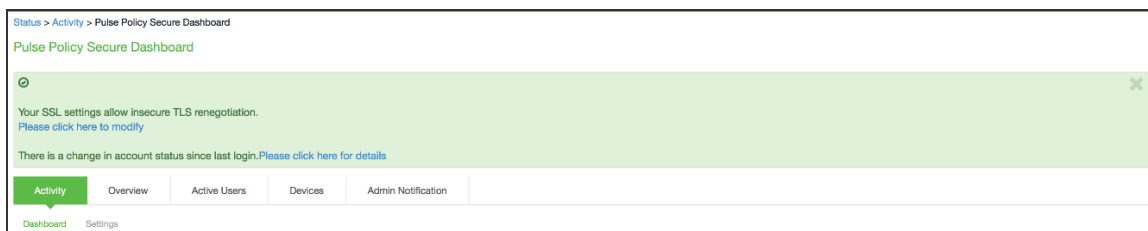
With JITC mode enabled, only the first match duplicate RADIUS policy found is reported in the error message.

Important Factors to Consider

Password Strengthening: When JITC is enabled, IPS does not allow an administrator to configure a password exactly same as previously configured 5 passwords. An error message is displayed in this case.



Notification for Unsuccessful Admin Login Attempts: With JITC Mode on, IPS shows a banner with the count of unsuccessful login attempts. This includes any change in the Admin status that would have happened since the last successful login. Upon clicking on the banner, the Administrator is directed to the status page, which provides more details about status or configuration change since last login. These configuration changes are cleared before the next login so that admin can see different set of configuration changes, if anything happened from the last login.



Re-authentication of Admin Users: IPS will force the administrator to re-authenticate with IPS whenever the following conditions occur:

- Add Role
- Delete Role
- Modify the Role
- Delete the Realm
- Update the Realm
- During DPE (Dynamic Policy Evaluation)

Configuration Change Notification: For details about configuration changes and status information since last login, go to **System > Status > Admin Notification**.

Status > Admin Notification

Admin Notification

Activity Overview Active Users Devices Admin Notification

▼ Login Status
Number of failed login attempts since last login : 0

▼ Role Status
Newly Added Roles :
Deleted Roles : admin2

Modified Roles

Role Name	Role Configuration Item	Changed From	Changed To
admin1	System Status	Write	Read
admin1	System Config	Write	Read
admin1	System Network	Write	Read
admin1	System Clustering	Write	Read
admin1	System IFMAP	Write	Read
admin1	System Dashboard	Write	Read

NDcPP Mode Option

NDcPP mode can be enabled in the Inbound tab with a checkbox. This status is also applied over to the Outbound tab. Turning on NDcPP automatically turns on FIPS mode and disables SSL/TLS Version TLS1.0 and below. Also, NDcPP Mode allows to choose only 16 Ciphers under Custom Encryption Strength. Turning on the NDcPP checkbox selects all the NDcPP ciphers by default on both, the Inbound and Outbound sides.



When the NDcPP Mode is enabled, backend server like Windows 2008 R2 which supports the SSL/TLS Version only till TLS1.0 cannot be connected.

syslog-ng server

Connection to syslog-ng server does NOT get established, since syslog-ng does not support TLSv1.1 and TLSv1.2.

rsyslog

Supports only till TLSv1.1. So, connection would not get established, if Outbound SSL Options is set to use TLSv1.2.

- To be NDcPP compliant, NTP Update Interval needs to be limited to 60 minutes. This is to avoid the potential drift becoming too excessive.
- For incoming client certificate during client certificate authentication and for incoming server certificate during backend syslog server connection 1024 bit Key Length is not allowed in both NDcPP and FIPS Mode where as SHA1 Signature Algorithm is not allowed only in FIPS Mode and is allowed in NDcPP Mode. This restriction is not applicable for Outgoing Certificates from IPS during SSL Negotiation.



Status > Admin Notification

Admin Notification

Activity Overview Active Users Devices Admin Notification

▼ Login Status
Number of failed login attempts since last login : 0

▼ Role Status

Newly Added Roles :
Deleted Roles : admin2

Modified Roles

Role Name	Role Configuration Item	Changed From	Changed To
admin1	System Status	Write	Read
admin1	System Config	Write	Read
admin1	System Network	Write	Read
admin1	System Clustering	Write	Read
admin1	System IFMAP	Write	Read
admin1	System Dashboard	Write	Read

Inbound Settings

When the NDcPP mode is enabled, the following settings appear by default in the Inbound SSL Options page:

- The Accept only TLS 1.1 and later is enabled by default in the Allowed SSL and TLS Version settings. Only the Accept only TLS 1.1 and Accept only TLS 1.2 options can be chosen. The Accept only TLS 1.0 and later and the Accept SSL V3 and TLS (maximize compatibility) are disabled. See figure
- With regards to the Allowed Encryption Strength settings the Custom SSL Cipher Selection is enabled by default with NDcPP Ciphers. All other options are disabled.

Inbound Settings

Allowed SSL and TLS Version
The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS. It is no longer supported.

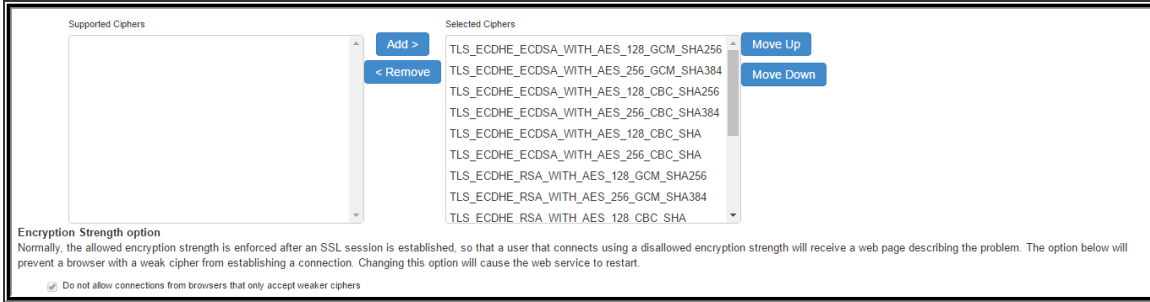
- Accept only TLS 1.2 and later (maximize security)
- Accept only TLS 1.1 and later
- Accept only TLS 1.0 and later
- Accept SSL V3 and TLS (maximize compatibility)

Allowed Encryption Strength
Strong ciphers (rated by the number of bits in the cipher) improve the security of SSL encryption, but some browsers may only support 40-bit ciphers. When there is more than one acceptable cipher, the Pulse Policy Secure will give preference to the cipher with the fastest data transfer rate, regardless of its relative encryption strength. Changing the encryption strength will cause the web service to restart. Please see the Setting Security Options section in the Admin guide for more details.

- PFS - Perfect Forward Secrecy
- SuiteB - Accept only SuiteB ciphers (Requires an ECC certificate)
- Maximize Security (High Ciphers)
- Maximize Compatibility (Medium Ciphers)
- Custom SSL Cipher Selection

The following is a list of Selected Ciphers in the Inbound Settings with the NDcPP mode enabled:

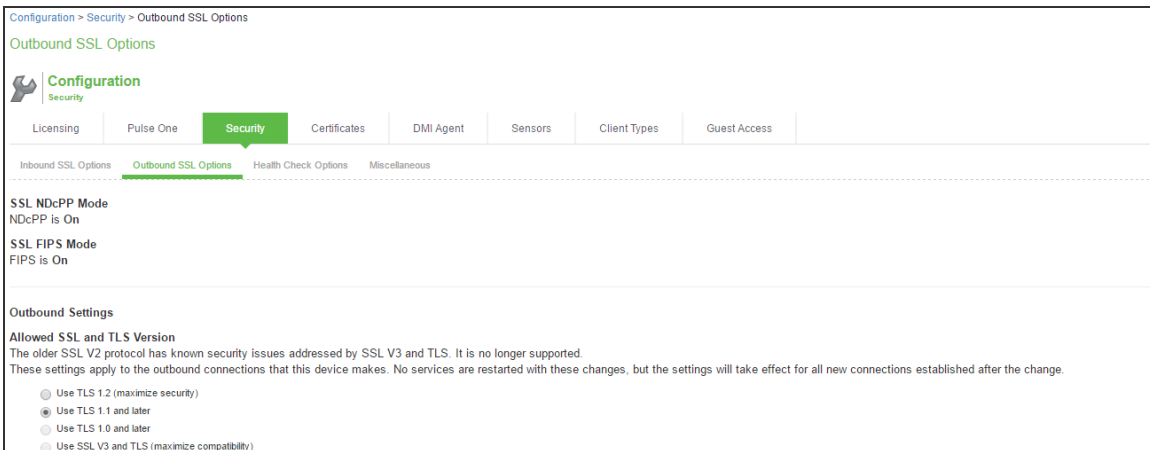
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384



Outbound Settings

When the NDcPP mode is enabled, the following settings appear by default in the Outbound SSL Options page:

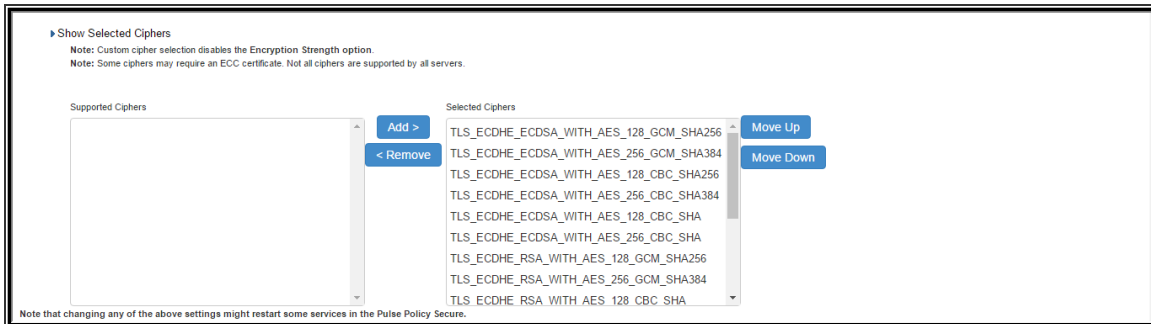
- The Accept only TLS 1.1 and later is enabled by default in the Allowed SSL and TLS Version settings. Only the Accept only TLS 1.1 and Accept only TLS 1.2 are editable. The Accept only TLS 1.0 and later and the Accept SSL V3 and TLS (maximize compatibility) are disabled.
- With regards to the Allowed Encryption Strength settings the Custom SSL Cipher Selection is enabled by default. All other options are disabled.
- Only the NDcPP ciphers configured in the Outbound SSL options settings are sent in the Outbound connections (IPS → backend SSL).



The following is a list of Selected Ciphers in the Outbound Settings with the NDcPP mode enabled:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384



Using the Management Port

This topic describes how to configure the management port. It includes the following information:

Management Port Overview

You connect the management port to an Ethernet switch or router that is part of your internal local area network (LAN) and that can connect to your network management infrastructure. When the management port is enabled, the following traffic is directed out the management port: archiving (FTP/SCP), NTP, push config, SNMP, syslog. When the management port is not enabled, that traffic uses the internal port.

Supported Platforms

The following hardware platforms are equipped with a management port: PSA Series

Configuring the Management Port

To configure the management port:

1. Select **System > Network > Management Port > Settings** to display the configuration page.
2. Complete the configuration as described in table.
3. Save your changes.

Network > Management > Management Port - Settings

Management Port - Settings

Network Settings
Management Port - Settings

Overview Internal Port External Port **Management Port** VLANs Routes Hosts Load Balancer

Settings ARP Cache ND Cache

Enter the network settings and click the Save Changes button at the bottom of the page.

Use Port

Enabled Disabled

When the management port is enabled, the following traffic is directed out the management port: syslog, SNMP traps, SNMP queries, NSM, NTP, FTP/SCP archiving and Push Config.

IPv4 Settings

*IP Address:

*Netmask:

*Default Gateway:

Note: If you need to specify static routes, you can do so on the [Static Routes](#) page.

IPv6 Settings

Enable IPv6 Disable IPv6

Note: Changing above setting might restart some services. This restart might drop all the connections to the Pulse Connect Secure.

Link Local Address:

*IPv6 Address:

*Prefix Length: (1 to 128)

*Default Gateway:

Advanced Port

MAC Address: 00:18:7D:22:48:C1

Link Speed:

*ARP Ping Timeout: seconds 3 to 300 seconds

*MTU: bytes Maximum Transmission Unit. If IPv6 is enabled (1280 to 1500), else (576 to 1500).


Default VLAN ID:

Default VLAN ID for the traffic for this port.
WARNING: Adding VLAN ID may break connectivity unless corresponding switch port is configured to handle tagged traffic.

Save Changes

Settings	Guidelines
Use Port?	
Use Port?	Select Enabled to use the port; otherwise, select Disabled.
IPv4 Settings	
IP Address	<p>Specify an IP address. An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.</p> <p>The format of an IPv4 address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0 to 255.</p>
Netmask	<p>A netmask indicates which part of an IP address indicates network identification and which part indicates the host identification. For example, the IP address and netmask 10.20.30.1 255.255.255.0 (or 10.20.30.1/24) refer to all the hosts in the 10.20.30.0 subnet. The IP address and netmask 10.20.30.1 255.255.255.255 (or 10.20.30.1/32) refer to a single host.</p>
Default Gateway	<p>Specify the IPv4 address for the default gateway for the routing domain to which the device belongs.</p> <p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p>
IPv6 Settings	
Enable IPv6 / Disable IPv6	<p>Disabled by default. Enable to support network management traffic over IPv6 networks.</p> <p>When you enable IPv6, the system acquires a link local address.</p> <p>If you switch from enabled to disabled, the system clears the link local address.</p>
Link Local Address	<p>Display the auto configured link local address (after you have enabled and saved the IPv6 configuration).</p>
IPv6 Address	<p>Specify a routable IPv6 address, such as a global unicast address that your network plan has provisioned for this host and interface. Automatic configuration methods are not supported. You must specify the appropriate address manually.</p>

Settings	Guidelines
Prefix Length	Specify how many of the higher-order contiguous bits of the IPv6 address comprise the prefix (the network portion of the IPv6 address). The default is 64.
Gateway	Specify the IPv6 address for the default gateway for the routing domain to which the device belongs. A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.
Advanced Settings	
MAC Address	Display the MAC address for the interface.
Link Speed	Specify the speed and duplex combination for the interface. If you run SNMP_GET and then change the Link Speed value, you must wait at least 5 minutes after submitting the change before running SNMP_GET again.
ARP Ping Timeout	(IPv4 only.) Specify how long the system should wait for responses to Address Resolution Protocol (ARP) requests before timing out. Cluster nodes send ARP requests to the gateways of other nodes to determine if they are properly communicating with one another. If you have not deployed a cluster, the system does not use this setting. If the node belongs to a cluster, the timeout interval that you specify is synchronized across the cluster. In multisite clusters, you can override this setting for the individual nodes in the cluster using options in the System > Clustering page. Use caution when changing this setting in active/passive clusters, however, because the system also uses the ARP Ping Timeout setting on the Internal tab as a failover timer for the VIP.
MTU	Specify the maximum transmission unit. If IPv6 is enabled, the valid range is 1280 to 1500. If IPv6 is not enabled, the valid range is 576 to 1500. We recommend you retain the default MTU setting (1500) unless you must change the setting for troubleshooting purposes.
Default VLAN ID	(Optional) Specify the default VLAN ID for the traffic of this port. When this parameter is set, all the traffic on this interface is subsequently tagged with the set VLAN ID and also accepts only incoming traffic with the same tag. Necessary changes are required on the connected switch port to handle bi-directional tagged traffic.

Settings	Guidelines
	<ul style="list-style-type: none"> - If default VLAN ID is set incorrectly or the connected switch port is not configured accordingly, the interface can become unreachable. - Default VLAN ID cannot be set if IPv6 is enabled. - Default VLAN ID is not supported in a clustered environment.  - In case of VMware ESXi based Virtual Appliance(VA), set the vSwitch configuration to port 4095 to allow IPS to tag the traffic. - The set default VLAN ID should be added as a member in the physical port of switch and the same VLAN should be removed from native VLAN ID.

Using the Serial Console to Configure the Management Port

To configure management port network settings from the serial console:

1. Start a serial console session.
2. Select item 1, System Settings and Tools.
3. Select item 10, Configure Management port. The text indicates if the option is enabled or disabled.
4. Enter the network settings for the Management Port, as prompted.



If you enable the Management Port but neglect to configure the IP address and netmask, the port reverts to a disabled state. Also, you cannot clear Management Port settings from the serial console when the port is disabled, though you can clear them from within the admin console.

5. When prompted to accept the changes, if they are correct, enter `y`. Otherwise, repeat the process to correct the settings.
6. Close the serial console.

Configuring Administrator Access

You can configure the **Administrators > Admin Realm > Authentication Policy > Source IP restrictions** configuration to enable administrator sign-in through the management port.

You can use Administrator realms to control administrator access to system ports, including the management port.

To control administrator access to the management port:

Enable the management port.

1. Perform one of the following steps:
 - Select **Administrators > Admin Realms > Admin Users** to modify the default admin users realm.
 - Select **Administrators > Admin Realms**, then click **New**, to create a new administrator realm.
2. Select the Authentication Policy > Source IP.
3. Select one of the following options:
 - **Allow users to sign in from any IP address**—Allows users to sign in from any IP address to satisfy the access management requirement.
 - **Allow or deny users from the following IP addresses**—Specifies whether to allow or deny users access from all the listed IP addresses, based on their settings.

To specify access from an IP address:

- Enter the IP address and netmask.
 - Select either Allow to allow users to sign in from the specified IP address, or Deny to prevent users from signing in from the specified IP address.
4. Select the available options to allow administrators to sign in to all available ports, to the management port or the internal port only, or to restrict them from signing in to any of the ports. In some cases, you may inadvertently limit administrative access completely. If this occurs, you can reconfigure the ports by way of the serial console.

5. Select from the following available options:

- Enable administrators to sign in on the management port.
- Enable administrators to sign in on the internal port.
- Enable administrators to sign in on the external port.

Admin Realm > Admin Users > Authentication Policy > Source IP

Source IP

General Authentication Policy Role Mapping

Source IP Browser Certificate Password Host Checker Lists

Allow users to sign in from any IP address
 Allow or deny users from the following IP addresses:

Delete [Add] [Remove]

IPv4/v6 Address	Netmask/Prefix Length	Allow/Deny	
<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> Allow <input type="radio"/> Deny	<input type="button" value="Add"/>
<input type="text"/>	<input type="text"/>		
<input type="text"/>	<input type="text"/>		

Note: This restriction will not be enforced if no IP addresses are listed. Add one or more source IP addresses from which users are allowed to sign in or denied access.

Administrator sign in ports

External Port is not enabled
Management Port is not enabled
 Enable administrators to sign in on the Management Port
 Enable administrators to sign in on the Internal Port
 Enable administrators to sign in on the External Port

Configuring VLAN Ports

Your network design might include VLANs to provide network segmentation. When connected to a trunk port on a VLAN-enabled switch, the system encounters traffic from all VLANs. This is useful for network designs with separate VLANs for separate classes of users or endpoints, and for making the system accessible from all VLANs. You can use RADIUS attributes to place different users in different network segments.

The system supports IEEE 802.1Q VLAN tagging. You must define a VLAN port for each VLAN. The internal port must be assigned to the root system and must be marked as the default VLAN. Routes to servers reachable from the VLAN interfaces must have the next-hop gateway set to the configured gateway for the VLAN interface, and must have the output port defined as the VLAN port.

When you save the configuration for a new VLAN port, the system creates two static routes by default:

- The default route for the VLAN pointing to the default gateway.
- The interface route to the directly connected network.

To configure a VLAN port:

1. Select **System > Network > VLANs**.
2. Click **New Port** to display the configuration page.
3. Complete the configuration as described in table.
4. Save your changes.

Settings	Guidelines
Use Port?	
Use Port?	Select Enabled to use the port; otherwise, select Disabled.
VLAN Settings	
Port Name	Specify a name that is unique across all VLAN ports that you define on the system or cluster. Only alphanumeric characters, "-", or "_" are allowed.
VLAN ID	Specify a number between 1 and 4094. The VLAN ID assignment must be unique on the system.
IPv4 Settings	

Settings	Guidelines
IP Address	<p>Specify an IP address and netmask combination that is from the same network as the VLAN. VLAN IP addresses must be unique. You cannot configure a VLAN to have the same network as the internal port. For example, if the internal port is 10.64.4.30/16 and you configure a VLAN as 10.64.3.30/16, you might get unpredictable results and errors.</p> <p>The format of an IPv4 address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0 to 255.</p>
Netmask	<p>Specify a netmask. A netmask indicates which part of an IP address indicates network identification and which part indicates the host identification. For example, the IP address and netmask 10.20.30.1 255.255.255.0 (or 10.20.30.1/24) refer to all the hosts in the 10.20.30.0 subnet. The IP address and netmask 10.20.30.1 255.255.255.255 (or 10.20.30.1/32) refer to a single host.</p>
Default Gateway	<p>Specify the IPv4 address for the default gateway for the routing domain to which the device belongs.</p> <p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p>
IPv6 Settings	
IPv6 settings	<p>Select Enable IPv6 to use the port; otherwise, select Disable IPv6.</p>
IPv6 Address	<p>Specify a routable IPv6 address, such as a global unicast address that your network plan has provisioned for this host and interface. Automatic configuration methods are not supported. You must specify the appropriate address manually.</p>
Prefix Length	<p>Specify how many of the higher order contiguous bits of the IPv6 address comprise the prefix (the network portion of the IPv6 address). The default is 64.</p>
Default Gateway	<p>Specify the IPv6 address for the default gateway for the routing domain to which the device belongs.</p> <p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p>

- Link speed, ARP ping timeout, and MTU settings are inherited from the internal port configuration.



- To configure an external VLAN port, Select System > Network > VLANs > External Port > New VLAN Port -Settings.

- To configure a Management port, Select System > Network > VLANs > Management Port > New VLAN Port -Settings.

Using Virtual Ports

Configuring Virtual Ports

You can use virtual ports to provide different groups of users access to the same system using different IP aliases and domains.

Virtual ports are associated with the physical internal port and physical external port. The virtual port shares all the network settings with the associated physical port, except for the IP address.

When you configure virtual ports, you are creating name-IP address pairs. The names and IP addresses must be unique in your network. An alias can include IPv4 addresses, IPv6 addresses, or both. However, the corresponding IP protocol must be enabled on the physical port for the addresses to take effect.

To configure a virtual port:

1. Select **System > Network > PortName > Virtual Ports**. PortName is Internal Port or External Port.
2. Click **New Port** to display the configuration page.
3. Complete the configuration as described in table.
4. Save your changes.

The screenshot shows the configuration page for a Virtual Port. The breadcrumb trail is: Network Settings > Internal Port > Virtual Ports. The page title is "Virtual Port". There are two tabs: "Virtual Ports" (active) and "ARP Cache". The configuration fields are:

- Name:** A text input field. A tooltip indicates: "Name of the virtual port. Only alphanumeric characters, '-', or '_' are allowed."
- Physical Port:** A dropdown menu with "Internal Port" selected. A tooltip indicates: "The physical port determines all characteristics of this virtual port other than IP address."
- IPv4 Address:** A text input field.
- IPv6 Address:** A text input field.

At the bottom, there are two buttons: "Save Changes" and "Cancel". A note at the bottom left states: "*Indicates required field".

Settings	Guidelines
Name	Specify a name for the virtual port. The names and IP addresses in the virtual port configuration must be unique in your network.
Physical Port	Display the name of the physical port associated with the virtual port. The virtual port inherits link speed, ARP ping timeout, and MTU settings from the physical port configuration.
IPv4 Address	Specify an IPv4 address. An alias can include IPv4 addresses, IPv6 addresses, or both. However, the corresponding IP protocol must be enabled on the physical port for the addresses to take effect.
IPv6 Address	Specify an IPv6 address. An alias can include IPv4 addresses, IPv6 addresses, or both. However, the corresponding IP protocol must be enabled on the physical port for the addresses to take effect.

Using Device Certificates with Virtual Ports

Virtual ports can be used to create multiple fully qualified domain names for user sign-in. When a user tries to sign in using the IP address defined in a virtual port, the system presents the certificate associated with the virtual port to initiate the SSL transaction.

You can approach the digital certificate security and virtual ports implementation in either of the following ways:

- Associate all hostnames with a single certificate**—With this approach, you use a single wildcard certificate to validate the identity of all system hostnames, regardless of which hostname is used to sign in. A wildcard certificate includes a variable element in the domain name, making it possible for users who sign in from multiple hosts to map to the “same” domain. For example, if you create a wildcard certificate for *.yourcompany.com, the system uses the same certificate to validate its identity to users who sign in to employees.yourcompany.com as it does to users who sign into partners.yourcompany.com.

- **Associate each hostname with its own certificate**—With this approach, you associate different hostnames with different certificates. Create a virtual port for each hostname. A virtual port activates an IP alias on a physical port. For example, you can create two virtual ports on a single appliance, mapping the first virtual port to the IP address 10.10.10.1 (sales.yourcompany.com) and the second virtual port to the IP address 10.10.10.2 (partners.yourcompany.com). Then you can associate each of these virtual ports with its own certificate, ensuring that users authenticate through different certificates.

To associate certificates with virtual ports:

1. Create virtual ports.
2. Import the device certificates.
3. Associate the device certificates with the virtual ports:
4. Select **System > Configuration > Certificates > Device Certificates**.
5. Click the link of the device certificate you want to configure to display the configuration page.
6. Use the controls in the “Present certificate on these ports” section to associate ports with the certificate.

Configuring the System Date and Time

You can use the admin console to set the system date and time manually or by configuring a network time protocol (NTP) server. The system supports NTPv4, which is backwards compatible with NTPv3 and NTPv2.

BEST PRACTICE: We recommend you use NTP to synchronize the date and time clocks on all network systems. Using NTP obviates issues that might occur with cluster synchronization, network communication that uses time-sensitive protocols, such as SAML, and implementation of time-based policies, such as local authentication server account expiration. In addition, using NTP as a standard in your network rationalizes timestamps in logs, which facilitates reporting and troubleshooting.

On a VMware virtual appliance, the data may be erased each hour if the same NTP server is not defined on the license server, and on the ESXi server.

To set the system date and time:

1. Select **System** > **Status** > **Overview** to display the System Status dashboard.

2. Click the **System Date and Time Edit** link to display the configuration page.

Status > Overview > Date and Time

Date and Time

System Date: 7/14/2020
System Time: 5:41:46 PM

Time Zone: (GMT+05:30) Kolkata, Chennai, Mumbai, New Delhi

▼ Time Source

Use Pool of NTP Servers

Configure pool of NTP servers (IP Address/Hostname)
Please make sure NTP server is reachable via port configured at [Advanced Networking](#) page.
For troubleshooting use ntpq command under [Troubleshooting](#) page

* NTP Server 1:	<input type="text" value="time.pool.ntp.org"/>	Key 1:	<input type="text" value="*****"/>	(optional)
NTP Server 2:	<input type="text" value="10.0.0.105.1"/>	Key 2:	<input type="text"/>	(optional)
NTP Server 3:	<input type="text" value="0.pool.ntp.org"/>	Key 3:	<input type="text" value="*****"/>	(optional)
NTP Server 4:	<input type="text" value="1.pool.ntp.org"/>	Key 4:	<input type="text"/>	(optional)

Set Time Manually

Date: (mm/dd/yyyy)

Time: AM (hh:mm:ss)

For troubleshooting, navigate to **Maintenance > Troubleshooting > Tools > Commands** and then use ntpq command.

Troubleshooting > Tools > Commands

Commands

User Sessions | Monitoring | **Tools** | System Snapshot | Remote Debugging

TCP Dump | **Commands** | Kerberos | Licensing Protocol Trace

Command:

Interface: Internal Port External Management Port

VLAN Port:


Output:

```

remote          refid          st t when poll reach  delay  offset jitter
-----
-vf2.bbnx.net   2022-11-17T18:28:28.103 2 u  50  64  337 261.339  8.645 24.610
*10.00.74.102  10.00.74.102 2 u  42  64  377  0.266 -1.354  0.558
+ntp1.doctor.com 50.205.244.28 2 u  52  64  377 213.809  0.763  6.402
+time.cloudflare 10.254.1.15 3 u  48  64  377  40.140  0.443  2.447
    
```

Operation complete

- Complete the configuration as described in table.
- Save the configuration.

Settings	Guidelines
Time Zone	Select your time zone. Selecting the appropriate time zone enables the system to automatically adjust the time for Daylight Saving Time changes.
Time Source	
Use Pool of NTP Servers	<p>Select this option to configure pool of NTP servers. Configuring one NTP server is mandatory and keys are optional.</p> <hr/> <p> IPS VM's deployed on VMWare ESX server will synchronize time with ESXi host. To use NTP/local time, turn off VMWare Tools Time Synchronization completely.</p> <hr/> <p>BEST PRACTICE:</p> <ul style="list-style-type: none"> It is not recommended to use only two NTP servers.

Settings	Guidelines
	<ul style="list-style-type: none"> If more than one NTP server is required, four NTP servers is recommended minimum. Four servers protects against one incorrect timesource.
NTP Server (s)	Specify the fully qualified domain name or IPv4/IPv6 address for the NTP server.
Key(s)	<p>If you are using NTPv4, specify the symmetric key. The key must be pre-synchronized with the NTP server. For example, if you want to configure NIST's clock as the NTP server, you must request a key beforehand and have NIST send that key to you.</p> <p>The key for MD5 is in the following format: KeyNumber M KeyValue The key for SHA1 is in the following format: KeyNumber SHA1KeyValue</p>
Set Time Manually	
Date	Specify the date. You can click Get from Browser to automatically populate the Date and Time fields.
Time	Specify the time and select AM or PM.

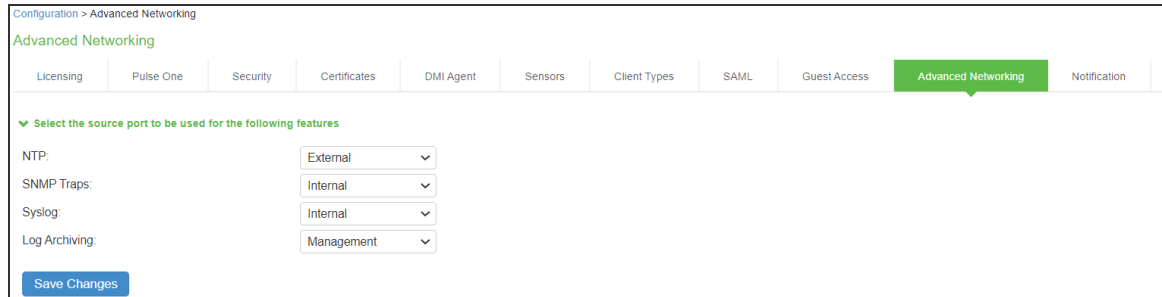
Configuring NTP and Other Services Traffic Over Any Physical Interface

The NTP, SNMP, Syslog, and Log archiving services are set to send the traffic through Management port by default. In case the Management port is not available, the traffic is routed through Internal port. Now, an administrator can modify the settings of NTP and other services to any physical interface.

The following procedure describes the steps to configure the ports for the services. Before you proceed, ensure the External and Management ports are enabled for use in the network settings.

To configure NTP and other Services:

1. Select **System > Configuration > Advance Networking**.
2. For the individual service, select the required port from the drop-down list.



The screenshot shows a web interface for configuring network services. At the top, there is a breadcrumb trail: Configuration > Advanced Networking. Below this, the page title is "Advanced Networking". A horizontal navigation bar contains several tabs: Licensing, Pulse One, Security, Certificates, DMI Agent, Sensors, Client Types, SAML, Guest Access, Advanced Networking (which is highlighted in green), and Notification. Below the navigation bar, there is a section titled "Select the source port to be used for the following features". This section contains four rows, each with a label and a dropdown menu:

Feature	Selected Port
NTP:	External
SNMP Traps:	Internal
Syslog:	Internal
Log Archiving:	Management

At the bottom left of the configuration area, there is a blue button labeled "Save Changes".

In a cluster environment, when a node joins the cluster, configuration of the node is replaced with the configuration of other nodes in the cluster.

Configuring Network Services

You configure DNS and WINS services when you initially configure the system with the serial console. If necessary, you can use the System > Network > Overview page to modify the configuration. You can also use this page to configure a hostname.

The network services overview page also displays the node name (if the node belongs to a cluster), and the status and interface statistics for the internal port, external port, and management port.

To configure network services:

1. Select **System > Network > Overview** to display the configuration page.
2. Complete the configuration as described in table.

3. Save your changes

The screenshot shows the 'Network Settings' page with the following sections:

- Status:** Internal Port (Connected, Speed: 10000Mb/s), External Port (Disabled), and Management Port (Connected, Speed: 10000Mb/s). It displays statistics for Rx/Tx Packets, Errors, Drops, and Multicast.
- Network Identity:** Hostname field with a placeholder 'Pluvvv92' and a note: 'Fully-qualified hostname (example: device.domain.com)'.
- DNS name resolution:** Primary DNS, Secondary DNS, and DNS Domain(s) fields. Preferred DNS Response is set to IPv4. Port for DNS Traffic is set to Internal Port.
- Windows networking:** WINS field with a placeholder and a note: 'Name or IP address'.
- IPv6 Settings:** Two checkboxes: 'Disable ICMPv6 echo response for multicast echo requests' and 'Disable ICMPv6 destination unreachable response'.
- DSCP value:** A field with '0' and a note: '(Applied to the dscp field of all the IPv6 packets originated or forwarded from the device.)'
- Save Changes:** A blue button at the bottom left.

Settings	Guidelines
Status	
Status	Display interface statistics for the internal port, external port, and management port.
Network Identity	
Hostname	Specify a fully qualified hostname. For example, domain.company.com. The hostname cannot exceed 30 characters
DNS Name Resolution	
Primary DNS	Specify the IPv4/IPv6 address for the primary DNS server.
Secondary DNS	Specify the IPv4/IPv6 address for the secondary DNS server.

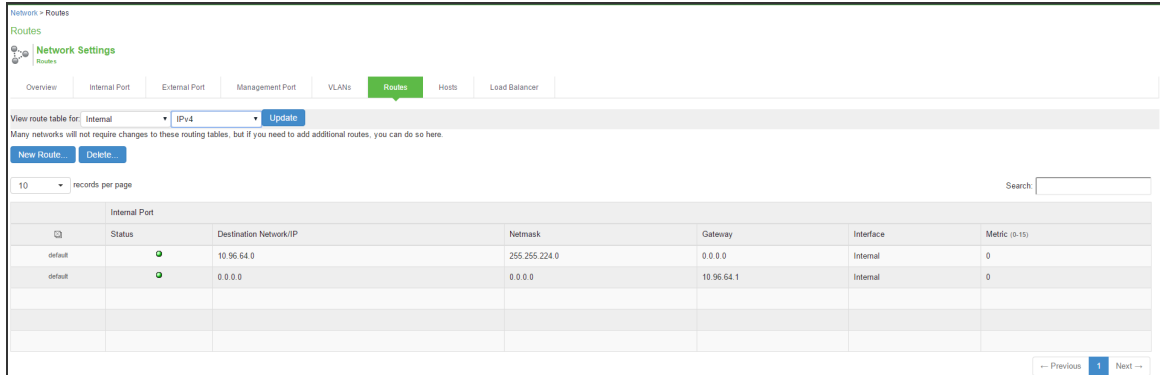
Settings	Guidelines
DNS Domain(s)	Specify a comma-separated list of default domains. The system searches the domains in the order they are listed.
Preferred DNS response	Determines the preferred DNS response from the DNS server. Select IPv4 if IPS sends and receives only IPv4 hostname resolution requests and responses from the DNS server. Select IPv6 if IPS sends and receives both IPv4 and IPv6 hostname resolution requests and responses from the DNS server.
Port for DNS Traffic	Administrator can modify the DNS setting to any physical interface namely Internal Port, External Port or Management Port. DNS port will be set to Internal port for fresh installation or an upgrade. The setting can be configured as node-specific or cluster-wide in case of a cluster.
Windows Networking	
WINS	Specify the hostname or IP address of a local or remote Windows Internet Naming Service (WINS) server that you use to associate workstation names and locations with IP addresses.

Managing the Routes Table

The system populates the routes table with dynamic, auto-discovered routes. Many networks will not require changes to this routing table. If necessary, you can delete routes or add static routes.

To manage the routes table:

1. Select **System > Network > Routes** to display the routes table.
2. Use the controls described in table to manage the routes table.



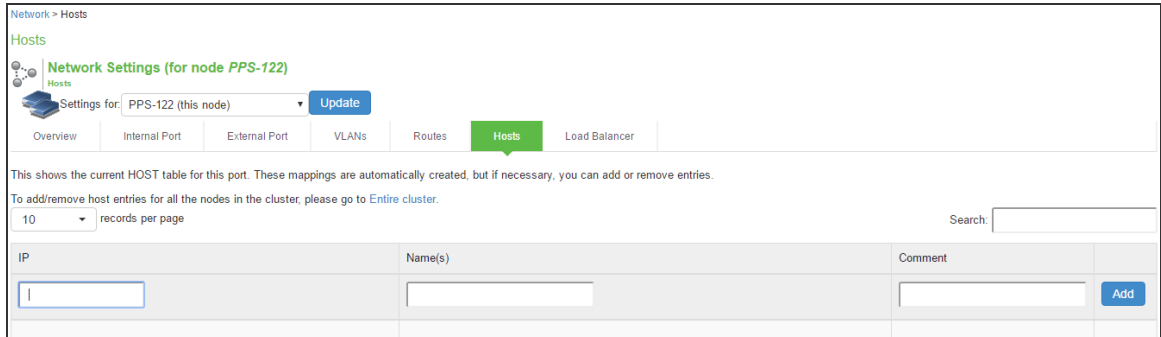
Controls	Description
View route table for	Use the controls to change the display to show the route table for internal, external, or management interfaces; and for IPv4 or IPv6 routes.
Delete	Select a row in the table and click Delete to delete a route.
New Route	Click New Route and complete the configuration to add a route to the table. You must specify a valid IP address, gateway, DNS address, and metric. The metric is a way of comparing multiple routes to establish precedence. Generally, the lower the number (from 1 to 15), the higher the precedence. Thus, a route with a metric of 2 is chosen over a route with a metric of 14. The metric value of zero (0) identifies the route as one that should not be used.

Managing the Hosts Table

In general, the system uses the configured DNS servers to resolve hostnames, but it also maintains a local hosts table that can be used for name resolution. The system populates some entries from host-IP address pair settings in your configuration. You can add host-IP address mappings for other hosts that might not be known to the DNS servers used by the system, or in cases where DNS is not reachable.

To manage the hosts table:

1. Select **System > Network > Hosts** to display the hosts table.



2. Use the controls described in table to manage the hosts table.

Controls	Description
Add	Specify an IP address, hostname, and comment (a description for the benefit of system administrators), and click Add.
Delete	Click the delete icon in the last column to delete the row from the table.

Managing the ARP Table

ARP stands for Address Resolution Protocol. In IPv4 networking, network nodes use ARP to maintain information about peer network nodes. ARP is used to associate the Layer 3 IP address with a Layer 2 MAC address of neighboring peer nodes. The system maintains an ARP table with dynamic, cached entries, and you can add static entries if necessary. The system caches dynamic entries for up to 20 minutes. Dynamic entries are deleted during a reboot. Static entries are restored after a reboot.

To manage the ARP table:

1. Select **System > Network > Port > ARP Cache**. Port is the Internal Port, External Port, or Management Port tab.

Network > Internal > Internal Port - ARP Cache

Internal Port - ARP Cache

Network Settings
Internal Port - ARP Cache

Overview Internal Port External Port Management Port VLANs Routes Hosts Load Balancer

Settings Virtual Ports ARP Cache ND Cache

This shows the current ARP table for this port. These mappings are automatically created, but if necessary, you can add or remove entries.

Delete... Delete Dynamic Entries

	IP Address	Physical Address	Type	
	<input type="text"/>	<input type="text"/>		Add
<input type="checkbox"/>	10.204.88.1	00:1F:12:35:64:40	Dynamic	
<input type="checkbox"/>	10.204.89.92	00:10:DB:FF:10:07	Dynamic	
<input type="checkbox"/>	10.204.91.254	00:26:88:6E:CE:01	Dynamic	

2. Use the controls described in table to manage the ARP table.

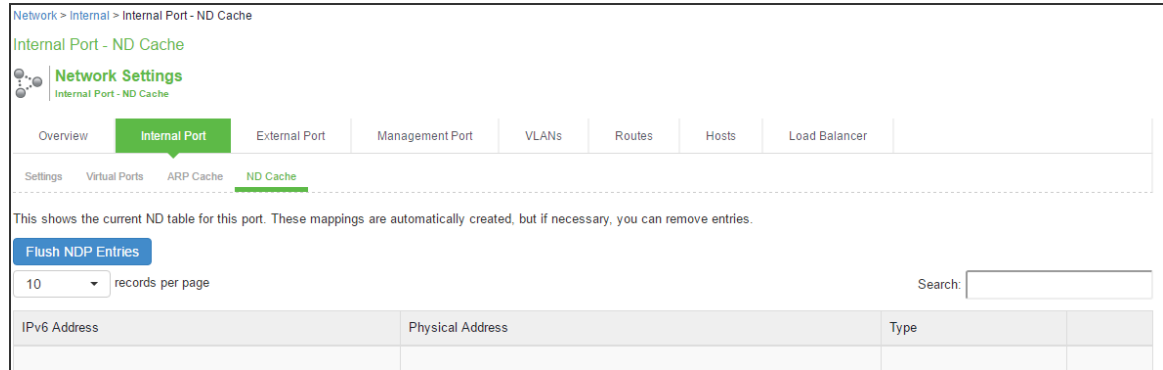
Controls	Description
Delete	Select a row in the table and click Delete to delete the entry.
Delete Dynamic Entries	Delete all dynamically discovered entries.
Add	Specify an IP address, a MAC address, and click Add to add an entry. If you add an entry that has the same IP address as an existing entry, the system overwrites the existing entry with your new entry.

Managing the Neighbor Discovery Table

In IPv6 networking, network nodes use the [Neighbor Discovery Protocol \(NDP\)](#) to determine the Layer 2 MAC addresses for neighboring hosts and routers. The system uses NDP to maintain a cache of neighboring routers that are reachable and can forward packets on its behalf.

To manage the neighbor discovery table:

1. Select **System > Network > Port > ND Cache**. **Port** is the Internal Port, External Port, or Management Port tab.
2. Select **Flush NDP Entries** to delete all dynamically discovered entries.



Configuring SSL Options

Use the System > Configuration > Security > SSL Options page to change the default security settings. We recommend that you use the default security settings, which provide maximum security, but you may need to modify these settings if your users cannot use certain browsers or access certain Web pages.

TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA cipher suites are supported. Both these ciphers use RSA for server authentication and ephemeral Diffie-Hellman (DHE) for key exchange. RSA server certificate is required for these ciphers. Only TLS_DHE_RSA_WITH_AES_256_CBC_SHA is available with the Accept 168-bit and greater option. In the Custom SSL Cipher configuration, TLS_DHE_RSA_WITH_AES_128_CBC_SHA is available only when AES-Medium is selected and TLS_DHE_RSA_WITH_AES_256_CBC_SHA is available only when AES-High is selected. Both ciphers are lower in priority over the other widely used cipher suites.

Enabling Granular Cipher Selection for Setting the Security Options

Granular cipher selection provides an administrator the ability to select specific ciphers and the preferred ordering of the selected ciphers. This feature also provides presets like Suite-B and PFS. There are two tabs, Inbound OpenSSL options and Outbound OpenSSL options. With this feature the administrator can select the ciphers that TLS/SSL connections will use. The Inbound OpenSSL options apply to all incoming connections. Outbound OpenSSL options apply to the following services:

- SCEP
- Syslog
- LDAPS
- Start TLS



FIPS Mode Settings is common for both Inbound and Outbound SSL Options.

A common cipher library has been added which can be used by both, the inbound and outbound connections. The outbound options are listed in a separate tab next to the inbound settings. The outbound settings have presets for High and Medium ciphers along with custom options. There is no PFS or SuiteB presets on the outbound side. From 5.3R3 release onwards, support for preset Low has been removed and the same can be configured using Custom SSL Cipher Selection option. For the SuiteB preset to work, IPS should have ECC Device Certificate mapped to Internal or External Port. SuiteB preset does not work if the ECC Device Certificate is mapped only to virtual port.

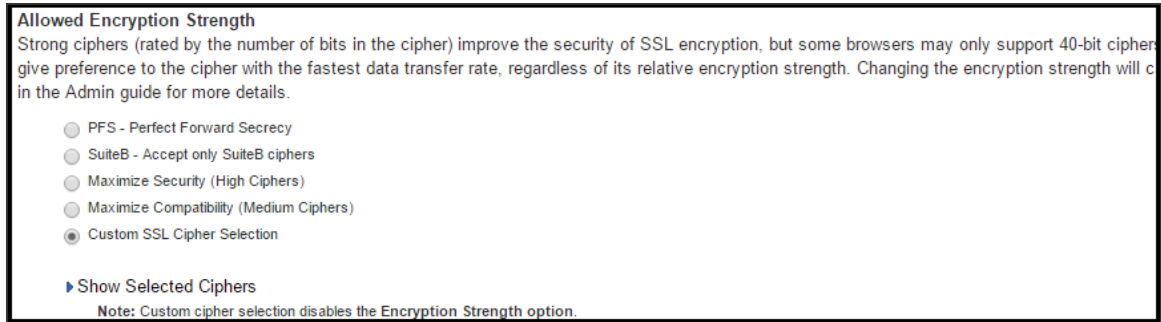
Enabling Inbound SSL Options

Only when FIPS mode is turned on, the FIPS compliant ciphers are available to be chosen from the Supported Ciphers panel. FIPS mode is editable only on the inbound option page.

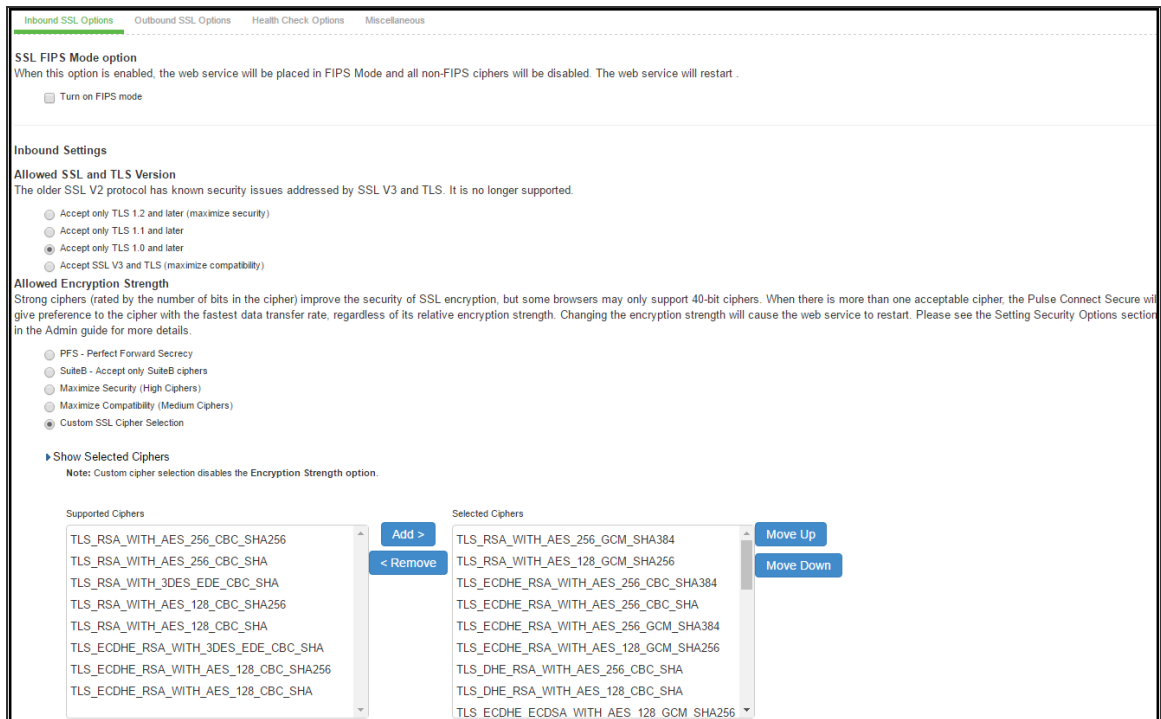
To set the security options with Inbound SSL options:

1. In the admin console, select **System > Configuration > Security > Inbound SSL Options**.

2. Under **Allowed Encryption Strength** choose **Custom SSL Cipher Selection**.

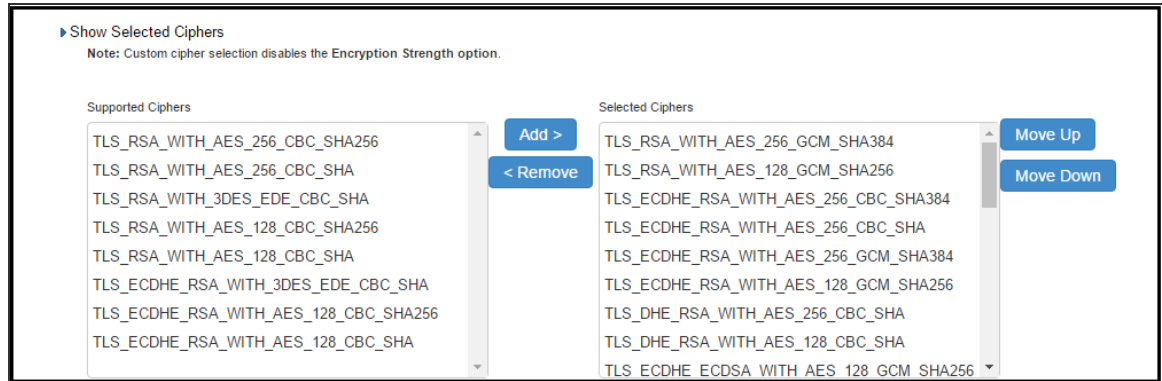


The two panels of Supported Ciphers and Selected Ciphers are displayed. Supported ciphers has the entire list of ciphers supported for the selected SSL or TLS version. Selected ciphers list the currently selected ciphers list. The below figure shows the two panels (Supported Ciphers and Selected Ciphers). Note that the Selected Ciphers and Supported Ciphers List will also be displayed for all Preset like PFS or SuiteB or Medium or High.



- To add a cipher, click the cipher string on the left panel and then click Add or double click the cipher name in the left panel.
- To remove the cipher, click the cipher name on the right panel and then click Remove or double click on the cipher name on the right side.

The selected ciphers on the right are listed in order of their priority from top to bottom. To change the priority of the ciphers, click on the cipher name and then click on Move Up to increase priority or the Move Down button to decrease the priority.



A list of the custom ciphers to be used on the device's port is displayed in the order the web server will select them. Note that Suite B ciphers are listed on top. End users who now log in to external virtual port p_ecdsa256 must have at least one of the listed ciphers installed on their browser or else they cannot log in to the server.

```

Configuration > Security > SSL Options
SSL Options

? Confirm Change to Custom Ciphers
Are you sure you want to use custom ciphers selection? If your browser does not support at least one of the ciphers listed below, you will not be able to continue.

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

```

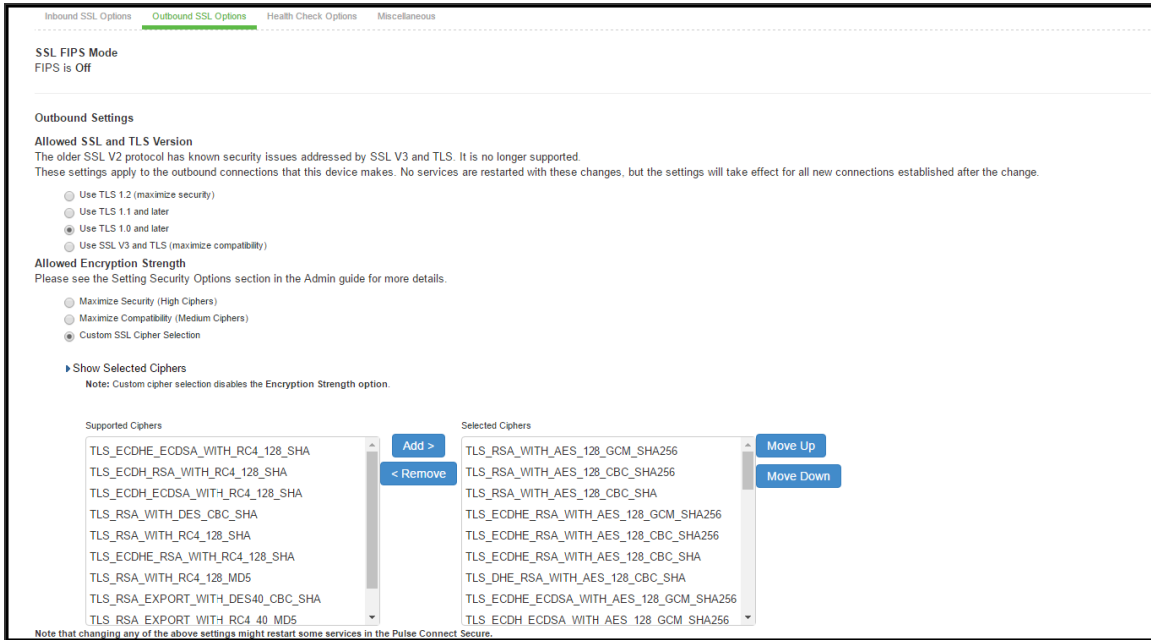
3. Click **Change Allowed Encryption Strength**.

When custom ciphers are selected, there is a possibility that some ciphers are not supported by the web browser. Also, if any of ECDH/ECDSA ciphers are selected, they require ECC certificate to be mapped to the internal/external interface. If ECC certificate is not installed, administrator may not be able to log in to the box. The only way to recover from this situation is to connect to the system console and select option 8 to reset the SSL settings from the console menu. Option 8 resets the SSL settings to its default. So, the previously set SSL settings are lost. This is applicable only to Inbound SSL settings.




Enabling Outbound SSL Options

We can configure non FIPS ciphers only for Outbound SSL Settings using Custom Cipher Selection option. There are options to change different SSL/TLS versions and different encryptions in the Outbound SSL Settings. The below figure shows the Outbound SSL Settings



Settings	Guidelines
SSL FIPS Mode option	Turn on FIPS mode— Select this option to enable FIPS mode.
Allowed SSL and TLS Version	Specify encryption requirements for clients. By default, the system requires SSL version 3 and TLS. The system honors this setting for all Web server traffic and all types of clients. You can require users who have older browsers that use SSL version 2 to update their browsers, or you can change this setting to allow SSL version 3, and TLS.
Allowed Encryption Strength	<ul style="list-style-type: none"> Accept only 168-bit and greater — If you select this option the system gives preference to 256-bit AES over 3DES. Accept only 128-bit and greater — (Default) If you select this option the system gives preference to RC4 ciphers. You can require users to have this level of encryption strength or change this default to an option compatible with the user base.

Settings	Guidelines
	<ul style="list-style-type: none"> • Accept 40-bit and greater — If you select this option the system gives preference to RC4 ciphers. Older browsers that predate the change in the U.S. export law in year 2000 that required 40-bit cipher encryption for international export, can still use 40-bit encryption. • Custom SSL Cipher Selection — Specify a combination of cipher suites for the incoming connection from the user's browser. If you select the AES/3DES option, the system gives preference to 256-bit AES over 3DES. <hr/> <p> When using 168-bit encryption, some Web browsers may still show 128-bit encryption (the gold lock on the browser status bar) even though the connection is 168-bit. This is typically a limitation of the browser's capability.</p> <hr/>
Encryption Strength option	The allowed encryption strength is enforced after an SSL session is established, so that a user connecting with a disallowed encryption strength receives a Web page describing the problem. Enable this option to prevent a browser with a weak cipher from establishing a connection.
SSL Handshake Timeout option	Determines the time elapse before the SSL handshake timeout. The default is 60 seconds.
SSL Legacy Renegotiation Support option	SSL and Transport Layer Security (TLS) renegotiations can be subjected to man-in-the-middle (MITM) attacks that can lead to abuse. A new TLS extension (defined in RFC 5746) ties renegotiations to the TLS connections they are being performed over to prevent these kinds of attacks. The SSL Legacy Renegotiation Support option is enabled by default and allows renegotiation between clients and servers even if they do not support the new TLS extension. Disable this option to not allow renegotiations between clients and servers that do not support the new TLS extension. A web server restart is required when you change the value of this option.

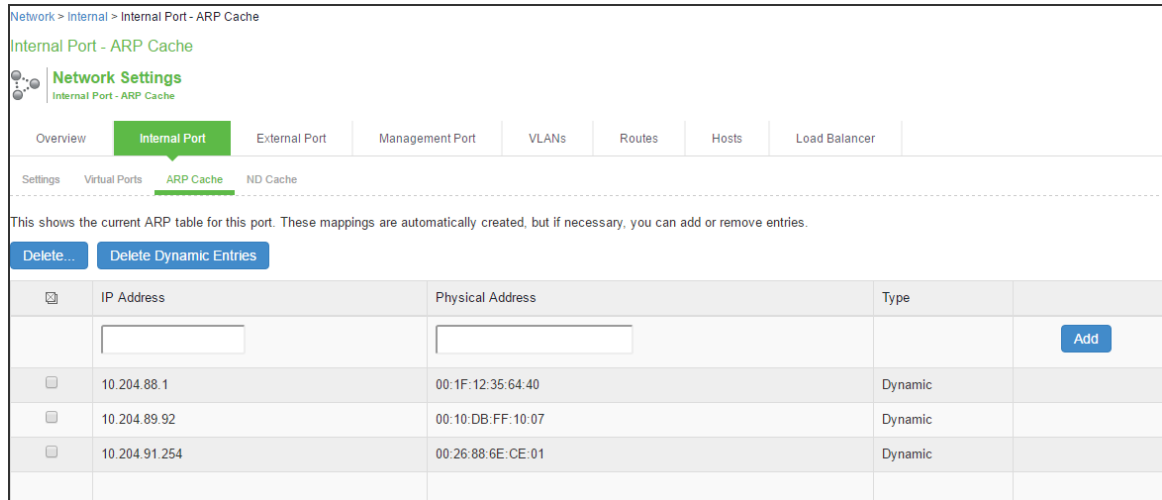
Configuring Health Check Options

You can use the **System > Configuration > Security > Health Check Options** page to configure the following security options:

- **Enable additional information via healthcheck.cgi**—This option is used by entities like load balancers to monitor the health status of the node.

To configure health check options:

1. Select **System > Configuration > Security > Health Check Options** to display the configuration page.



2. Select the Enable additional information via healthcheck.cgi checkbox and **Save Changes**. A URL parameter 'status' needs to be passed to get additional information to the health check URL. For more information about parameters such as CPU usage and number of active sessions use <https://<Ivanti Policy Secure>/dana-na/healthcheck/healthcheck.cgi?status=all>. For more information about SBR statistics use <https://<Ivanti Policy Secure>/dana-na/healthcheck/healthcheck.cgi?status=sbr>
3. Enter the IPv4/v6 address of the load balancer and click **Add**.
4. Click **Save Changes**.

Configuring Miscellaneous Security Options

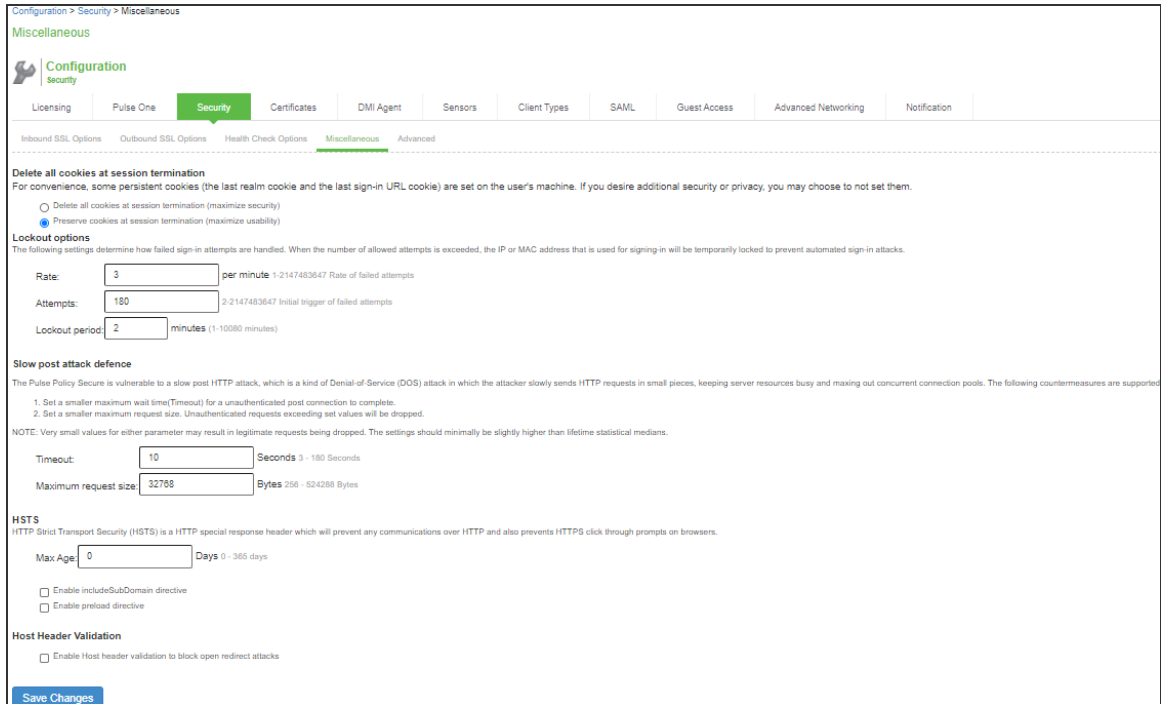
You can use the **System > Configuration > Security > Miscellaneous** page to configure the following security options:

- **Persistent cookie options**—Choose whether to preserve or delete persistent cookies when a session is terminated.

- **Lockout options**—You can configure lockout options to protect the system from denial of service (DoS), distributed denial of service (DDoS), and password-guessing attacks.

To configure cookie and lockout options:

1. Select **System > Configuration > Security > Miscellaneous** to display the configuration page.
2. Complete the configuration as described in table.
3. Save the configuration.



Settings	Guidelines
Delete all cookies at session termination	For convenience, the system sets persistent cookies on the user’s machine to support functions such as multiple sign-in, last associated realm, and the last sign-in URL. For additional security or privacy, you can choose not to set them.
Lockout options	
Rate	Specify the number of failed sign-in attempts to allow per minute.

Settings	Guidelines
Attempts	Specify the maximum number of failed sign-in attempts to allow before triggering the initial lockout. The system determines the maximum initial time (in minutes) to allow the failed sign-in attempts to occur by dividing the specified number of attempts by the rate. For example, 180 attempts divided by a rate of 3 results in an initial period of 60 minutes. If 180 or more failed sign-in attempts occur within 60 minutes or less, the system locks out the IP address being used for the failed sign-in attempt.
Lockout period	Specify the length of time (in minutes) the system must lock out the IP address.
Slow Post Attack Defence	
Timeout	By default, the POST body is received within 10 seconds. If the browser is unable to send the POST body within 10 seconds the connection is eventually dropped. (Configurable from 3 - 60Sec)
Maximum Request Size	By default, now a connection is directly rejected if it tries to POST more than 4KB in POST body (Configurable from 256 Bytes to 24 KB)
HSTS	
Max Age	Specify the maximum age for HSTS. It can be disabled by configuring max age as 0.
Enable include Subdomain directive	Select the check box to enable/disable the include Subdomain directive. By default, it is turned off.
Enable preload directive	Select the check box to enable/disable the preload directive. By default, it is turned off.
Host Header Validation	
Enable Host Header Validation	Select the check box to enforce Host Header validation. By default, it is turned off. When Host header validation is enabled, every http request will be validated against hostnames

Settings	Guidelines
to block open redirect attacks	and IP v4/v6 addresses known to the IPS server. If match is not found, the request will be dropped.

Scenario Illustrating Lockout Settings Workflow

The following scenario illustrates how lockout settings work. For example, assume the following settings:

- **Rate** = 3 failed sign-in attempts per minute
- **Attempts** = 180 maximum allowed in initial period of 60 minutes (180/3)
- **Lockout period** = 2 minutes

The following sequence illustrates the effect of these settings:

- During a period of 3 minutes, 180 failed sign-in attempts occur from the same IP address. Because the specified value for Attempts occurs in less than the allowed initial period of 60 minutes (180/3), the system locks out the IP address for 2 minutes (fourth and fifth minutes).
- In the sixth minute, the system removes the lock on the IP address and begins maintaining the rate of 3 failed sign-in attempts/minute. In the sixth and seventh minutes, the number of failed sign-in attempts is 2 per minute, so the system does not lock the IP address. However, when the number of failed sign-in attempts increases to 5 in the eighth minute, which is a total of 9 failed sign-in attempts within 3 minutes, the system locks out the IP address for 2 minutes again (ninth and tenth minutes).
- In the eleventh minute, the system removes the lock on the IP address and begins maintaining the rate of 3 failed sign-in attempts per minute again. When the rate remains below an average of 3 per minute for 60 minutes, the system returns to its initial monitoring state.

Configuring Custom HTTP Headers

Ivanti Policy Secure (IPS) supports several HTTP headers, which are sent in response to the client request. There are several more headers built to improve security and prevent attacks like XSS. The Custom HTTP Headers configuration enables the administrator to add new headers that they want to enforce.

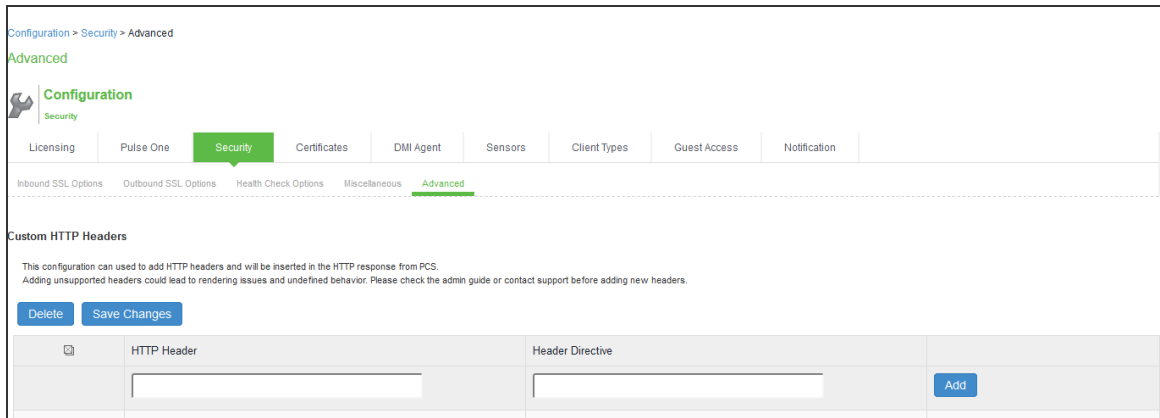
To configure custom HTTP header:

1. Select **System > Configuration > Security > Advanced**.
2. In the Custom HTTP Headers section, enter the HTTP header name and the directives along with the values.
3. Click **Add**.
4. Multiple headers can be added or removed. After adding the headers, click **Save Changes**.



- Administrator should ensure the correctness of the values that they enter, as the system validation on the input values is limited

- If the administrator configured HTTP header seems to affect the way the page is rendered or is locked out, use the console option to reset the custom HTTP header values.



The following table lists the OWASP recommended headers.

Header	Need IPS Web Server Changes	Supported Browsers
HPKP	Yes	Firefox, Chrome, Opera
X-XSS-Protection	No	Chrome and IE
X-Content-Type-Options	No	Firefox, Chrome, Opera and IE
Content-Security-Policy	Yes	All major browsers

Header	Need IPS Web Server Changes	Supported Browsers
X-Permitted-Cross-Domain-Policies	Yes	Not supported
Referrer-Policy	No	Chrome, Firefox and Opera
Expect-CT	No	Chrome and Opera
Feature-Policy	No	Not supported
HSTS	No	
X-Frame-Options	No	

Using the Serial Port

This topic describes use of the serial port and serial port console. It includes the following information:

Connecting to the Serial Port Console

In cases where the admin console is unavailable, you can perform network and host configuration tasks and troubleshooting using the serial port console.

To connect to the serial console:

1. Plug a null modem crossover cable from a console terminal or laptop into the device serial port. This cable is provided in the product box. Do not use a straight serial cable.
2. Configure a terminal emulation utility, such as HyperTerminal, with the following serial connection parameters:
 - 9600 bits per second
 - 8-bit No Parity (8N1)
 - 1 Stop Bit
 - No flow control


```

C:\> Telnet termsrv

Current version: 5
Reset version: 5

Please choose from among the following options:

 1. Network Settings and Tools
 2. Create admin username and password
 3. Display log
 4. System Operations
 5. Toggle password protection for the console (Off)
 6. Create a Super Admin session.
 7. System Snapshot

Choice: _

```

Options	Description
1. Network Settings and Tools	Enables you to change standard network settings; print a routing table; print or clear an ARP cache; run the ping and traceroute commands, remove static routes, and add an ARP entry.
2. Create admin username and password	Enables you to create a new super administrator account.
3. Display log	Enables you to display system configuration, user access logs, or administrator access logs through the serial console. Note that must enter q to return to serial console options after viewing the logs.
4. System Operations	Enables you to reboot, shut down, restart, roll back, or factory reset the system without using the admin console.
5. Toggle password protection for the console	Enables you to password protect the serial console. When you toggle this option to "on," only super administrators are allowed access.
6. Create a Super Admin session	Enables you to create a recovery session to the admin console, even if you have configured the system to block access to all administrators. When you select this option, the system generates a temporary token that is valid for 3 minutes. Enter the following URL into a browser window: https://<fully-qualified-domain-name>/dana-na/auth/recover.cgi

Options	Description
	<p>Then, enter the temporary token when prompted to sign in to the admin console.</p> <p>When you select this option, the system blocks any additional administrators from signing in to the admin console until you sign in to the specified URL and initiate a session using your token. The appliance blocks additional sign-in attempts so that you can fix any configuration problems that the system may have encountered without conflicting with another session.</p>
7. System Snapshot	<p>Enables you to take a system snapshot without using the admin console. When you select this option, the system takes the snapshot immediately. You can then send the snapshot file, by way of SCP, to a remote system. The system prompts you for the destination server port, user ID, password, and the destination path to the remote directory.</p> <p>If you choose not to send the snapshot file to a remote system, the system saves the file locally. The next time you log in to the admin console, the System Snapshot tab contains a link to the snapshot file.</p>

Using the Serial Console to Roll Back to a Previous OS Version

You can use the admin console to roll back the configuration to a previous state. If the rollback option is not available in the admin console, you can use the procedure described in this section to perform the system rollback.

If you have not yet performed an OS service package upgrade, there is no previous state to roll back to, and the rollback option is not available. If you have performed an OS service package upgrade, any system and user configuration data created after the upgrade is lost unless you export the most current configuration files before rolling back the system and then import them afterwards.

To roll back to the previous OS service package:

1. Connect to the serial console.
2. In a browser window, sign in to the admin console.
3. Select **Maintenance > System > Platform**.
4. Click Reboot Now and then return to the console utility window. The window displays a message that the system is restarting.

5. After several moments, you are prompted to use the Tab key to select options. Press Tab, and when prompted for the configuration to load, type rollback and then press `Enter`.

After you click Reboot Now, the rollback status is output to the screen, and when complete, you are prompted to press Return (Enter) to modify system settings, which returns you to the initial setup options. When you are finished entering data, simply close the serial console window.

If you wait more than 5 seconds to enter your choice, the current system configuration is automatically loaded and you must go back to the admin console and click Reboot Now to start the process again. If you have already performed a system rollback, the rollback option is not available again until you upgrade the OS service package again.

Using the Serial Console to Reset the System to the Factory Image

In rare cases, you might need to reset the system to its original factory settings. Before performing this advanced system recovery option, contact PSGSC (<http://www.pulsesecure.net/support/>). If possible, export the most current system and user configuration data before performing a factory reset.

To perform a factory reset:

1. Connect to the serial console. In a browser window, sign in to the admin console.
2. Select **Maintenance > System > Platform**.
3. Click **Reboot** and then go back to the console utility window. The window displays a message that the system is restarting.
4. After several moments, you are prompted to use the Tab key to select options. Press Tab, and when prompted for the configuration to load, type factory-reset and then press `Enter`. If you wait more than 5 seconds to enter your choice, the current system configuration is automatically loaded, and you must go back to the admin console and click Reboot Now to start the process again.
5. When you are prompted to confirm performing a factory reset, type proceed and then press `Enter`. The system begins the process of resetting the machine to its original settings and outputs several screens of data. After several minutes, you are prompted to use the Tab key to select configuration choices.

When prompted to press the Tab key, do one of the following:

- Wait for the default selection (current) to start automatically.
- Press Tab, type current, and then press `Enter`.

You are then prompted to enter the initial configuration settings. For details on how to proceed, see the installation guide provided in the product packaging or on the Ivanti Global Support Center.

After you complete the initialization process, you can upgrade to the latest OS service package and import saved system and user configuration files to return to the last good working state of your system.

You might receive errors from the system during the initial setup or on a factory reset. Before the system starts services, it monitors the network port for a maximum of 120 seconds. The system checks the link status and sends ARP requests to the default gateway. If there is a problem, after 5 seconds, the system displays a message on the serial console that starts with `NIC:.....`. If the link recovers within 120 seconds, the startup process continues. If the link does not recover, the following message is displayed:

Internal NIC:.....[Down code=0x1]

- **0x1** means that the interface link status reported by the NIC remains off (for example, a disconnected cable or a cable is in the wrong port).
- **0x2** means that the gateway is unreachable. The system boots but is not reachable from IP addresses bound to that network port.

Certificate Security Administration

Understanding Digital Certificate Security

Ivanti Policy Secure(IPS) uses Public Key Infrastructure (PKI) to secure the data sent to clients over the Internet. PKI is a security method that uses public and private keys to encrypt and decrypt information. These keys are enabled and stored through digital certificates. A digital certificate is an encrypted electronic file issued by a certificate authority (CA) that establishes credentials for client/server transactions.

In public key cryptography, a public/private key pair is used to encrypt and decrypt data. Data encrypted with a public key, which the owner makes available to the public, can be decrypted with the corresponding private key only, which the owner keeps secret and protected. For example, if User1 wants to send User2 an encrypted message, User1 can encrypt it with User2's public key and send it. User2 then decrypts the message with the private key. The reverse process is also useful: encrypting data with a private key and decrypting it with the corresponding public key. This process is known as creating a digital signature. For example, if User1 wants to present their identity as the sender of a message, they can encrypt the message with her private key and send the message to User2. User2 then decrypts the message with User1's public key, thus verifying that User1 is indeed the sender.

IPS uses the following types of digital certificates to establish credentials and secure session transactions:

- Device certificates—A device certificate helps to secure network traffic to and from the Ivanti service using elements such as company name, a copy of your company's public key, the digital signature of the CA that issued the certificate, a serial number, and expiration date. In addition, IPS uses a device certificate for communications with the Infranet Enforcers.
- Trusted client CAs—A trusted client CA is a client-side certificate issued by a CA. You can use trusted client CAs in the access management framework realm and role configurations to require certificates or certificates with specific attributes. For example, you may specify that users must present a valid client-side certificate with the OU attribute set to "yourcompany.com" to sign into the Users authentication realm.
- Trusted server CAs—A trusted server CA is the certificate of a Web server that you trust. You can install a trusted server CA to validate the credentials of the web sites that users access through the Pulse Client service.

- Code-signing certificates—A code-signing certificate (also called an applet certificate) is a type of server-side certificate that re-signs Java applets that are intermediated by IPS. You can use the self-signed code-signing certificate that comes pre-loaded, or you can install your own code-signing certificate.
- Client Authentication certificates—The client auth certificate is used when backend SSL servers require IPS to present a client certificate.



- The system can verify certificates that use SHA2 as the message digest.
 - Only ECDSA certificates are supported other DSA certificates are not supported.
-

Using Device Certificates

This topic describes how to use device certificates. It includes the following information:

Understanding Device Certificates

A device certificate helps to secure network traffic to and from the Pulse Client service using elements such as your company name, a copy of your company's public key, the digital signature of the Certificate Authority (CA) that issued the certificate, a serial number, and an expiration date. The system also uses device certificates for secure communications with the Infranet Enforcer.

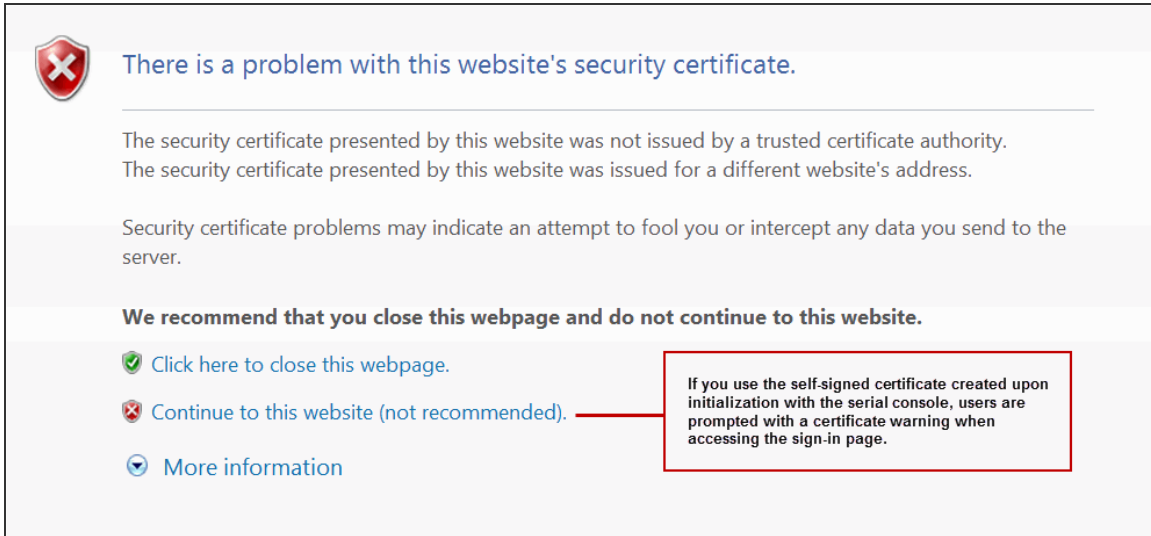
When receiving encrypted data from the system, the client's browser first verifies whether the device certificate is valid and whether the user trusts the CA that issued the certificate. If the user has not already indicated that they trust the certificate issuer, the Web browser prompts the user to accept or install the certificate.

The system supports X.509 device certificates in DER and PEM encode formats (file extensions include .cer, .crt, .der, and .pem) as well as PKCS #12 (file extensions include .pfx and .p12). The system also supports the following features:

- Intermediate device CA certificates—Within a certificate hierarchy, one or more intermediate certificates are branched off a single root certificate.
- Multiple device certificates—When using multiple device certificates, each certificate handles validation for a separate hostname or fully qualified domain name (FQDN) and can be issued by a different CA.

Understanding Self-Signed Certificates

When you initialize the system with the serial console, the system creates a self-signed certificate that enables you to immediately begin setting up the system. Users are prompted with a security alert each time they sign in because the certificate is not issued by a trusted CA.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority. The security certificate presented by this website was issued for a different website's address.


Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

- [Click here to close this webpage.](#)
- [Continue to this website \(not recommended\).](#)
- [More information](#)

If you use the self-signed certificate created upon initialization with the serial console, users are prompted with a certificate warning when accessing the sign-in page.

Before promoting the system to production use, we recommend you replace the self-signed certificate with a certificate issued by a trusted CA.

 In IPS deployments with ScreenOS Enforcers, you must use a CA-signed device certificate. If you use a self-signed certificate, the ScreenOS Enforcer does not allow a connection. Import a CA-signed device certificate into IPS, and then import the certificate of the CA that signed the device certificate into the ScreenOS Enforcer.

Importing a Device Certificate and Private Key

The system uses certificates to verify itself to other network devices. A digital certificate is an electronic means of verifying your identity through a trusted third party, known as a Certificate Authority (CA). Your company might use its own enterprise CA server, or it might use a reputable third-party CA.

To import an enterprise root server certificate and private key:

1. Select **System > Configuration > Device Certificates**.

Configuration > Certificates > Device Certificate

Device Certificate

Licensing | Pulse One | Security | **Certificates** | DMI Agent | Guest Access | Notification

Device Certificates | Trusted Client CAs | Trusted Server CAs | Client Auth Certificates | Certificates Validity Check

Specify the Device Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom [Intermediate CAs](#).

[Import Certificate & Key...](#) [Delete...](#)

10 records per page Search:

<input type="checkbox"/>	Certificate issued to	Issued by	Valid Dates	Used by
<input type="checkbox"/>	psecure.net	psecure.net	Oct 25 05:47:50 2018 GMT to Apr 16 05:47:50 2024	

2. Click **Import Certificate & Key** to display the configuration page.

Configuration > Certificates > Import Certificate and Key

Import Certificate and Key

Use one of the forms below to import an existing certificate and its corresponding private key. If the files are encrypted, you will also need to specify the password.

▼ If certificate file includes private key

Certificate File: [Browse](#) No file chosen
Password Key:
[Import](#)

▼ If certificate and private key are separate files

Certificate File: [Browse](#) No file chosen
Private Key File: [Browse](#) No file chosen
Password Key:
[Import](#)

▼ Import via System Configuration file

All Device Certificates and CSRs will be imported and added to the existing certificates and CSRs.

System Configuration File: [Browse](#) No file chosen
Password:
[Import](#)

- Use one of the following options to complete the import procedure:
 - If certificate file includes private key**—When the certificate and key are contained in one file. The file format is .pfx.
 - If certificate and private key are separate files**—When the certificate and key are in separate files.
 - Import via System Configuration file**—When the certificate and key are contained in a system configuration file. With this option, the system imports all the certificates specified (including private keys and pending CSRs, but not the corresponding port mappings).

In the appropriate form, browse to the certificate and key files. If the file is encrypted, enter the password key.

- Click **Import**.



The **Import Certificate** and **Key** button is disabled on FIPS hardware platforms because importing private keys is not allowed. On a FIPS hardware platform, you must create a CSR and then import a signed certificate from the CA.

Creating a Certificate Signing Request

If your company does not own a digital certificate for its Web servers, you can create a certificate signing request (CSR) and then send the request to a CA for processing. When you create a CSR, a private key is created locally that corresponds to the CSR. If you delete the CSR at any point, this file is also deleted, prohibiting you from installing a signed certificate generated from the CSR.

To create a certificate signing request:

- Select **System > Configuration > Certificates > Device Certificates**.
- Click **New CSR** to display the configuration page.
- Complete the required information and click **Create CSR**.
- Follow the onscreen instructions, which explain what information to send to the CA and how to send it.

When you submit a CSR to a CA authority, you might be asked to specify either the type of Web server on which the certificate was created or the type of Web server the certificate is for. Select apache (if more than one option with apache is available, select any). If you are prompted for the certificate format to download, select the standard format.

Do not send more than one CSR to a CA at one time. Doing so can result in duplicate charges.

Configuration > Certificates > New Certificate Signing Request

New Certificate Signing Request

Use this page to create a new Certificate Signing Request (CSR) to send to your Certificate Authority of choice.

Common Name:
(e.g., secure.company.com)

Organization Name:
(e.g., Company Inc.)

Org. Unit Name:
(e.g., IT Group)

Locality:
(e.g., SomeCity)

State (fully spelled out):
(e.g., California)

Country (2 letter code):
(i.e., US)

Email Address:

Key Type: RSA ECC

Key Length: bits

Please enter some random characters to augment the system's random key generator.
We recommend that you enter approximately twenty characters.

Random Data:
(used for key generation)

[Create CSR](#)



To view details of any pending requests that you previously submitted, click the Certificate Signing Request Details link.

Importing a Signed Certificate Created from a CSR

When you receive the signed certificate from the CA, import it.

To import a signed device certificate created from a CSR:

1. Select **System > Configuration > Certificates > Device Certificates**.
2. Under **Certificate Signing Requests**, click the **Pending CSR** link that corresponds to the signed certificate.
3. Under Import signed certificate, browse and select the certificate file you received from the CA, and then click **Import**.

✔ **CSR created successfully:** Your CSR was created successfully. See below for instructions on sending the CSR to a Certificate Authority. The certificate approval process may take several days. When you receive the signed certificate from the Certificate Authority, you will need to import the certificate to complete this process.

[Configuration](#) > Pending Certificate Signing Request

Pending Certificate Signing Request

CSR Details

Common Name: pulsesecure.net
 Created: 1/3/2017 10:50:24
 Org. Name: PulseSecure Locality: ??
 Org. Unit Name: ?? State: ??
 Email Address: ?? Country: ??
 Key Size: 1024 bits

[Back to Device Certificates](#)

Step 1. Send CSR to Certificate Authority for signing

To send the CSR to a Certificate Authority (CA), you need to copy the encoded text below, including the BEGIN and END lines, and submit it to the CA in one of the following ways:

- Save the text as a .cert file and attach it to an email message to the CA
- Paste the text into an email message to the CA
- Paste the text into a Web form provided by the CA

Note: Manage the CSR process carefully. If you submit more than one CSR to a CA, you may be billed for each CSR.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB8zCCAwwCAQAwdzELMAkGA1UEBhMCPz8xCzAJBgNVBAsMAj8/
MQswCQYDVQQH
DAI/PzEUMBIGA1UECgwLUHVsc2VTZW1cmUxCzAJBgNVBAsMAj8/
MREwDwYJKoZI
```

Step 2. Import signed certificate

When you receive the signed certificate file from the CA, select it below and click Import. This will add the signed certificate and remove this pending CSR.

Signed certificate: No file chosen

Understanding Intermediate Certificates

Within a certificate hierarchy, one or more intermediate certificates are branched off a single root certificate. The root certificate is issued by a root CA and is self-signed. Each intermediate certificate is issued by the certificate preceding it in the chain.

To use chained certificates in your deployment, you must ensure that the server and client (Web browser) together contain the entire certificate chain. For example, you can secure traffic using a chain that stems from a VeriSign root certificate. If your users' browsers come preloaded with VeriSign root certificates, you need to install only the lower-level certificates in the chain. When your users sign in, the system presents any required certificates within the chain to the browser to secure the transaction. The system creates the proper links in the chain using the root certificate's IssuerDN. If the system and browser together do not contain the entire chain, the user's browser does not recognize or trust the device certificate because it is issued by another certificate instead of by a trusted CA.

You can upload one or more intermediate CAs in a PEM file. The entire chain must be sent to the client in descending order, starting with the root certificate.

Within a certificate hierarchy, one or more intermediate certificates are branched off a single root certificate. The root certificate is issued by a root CA and is self-signed. Each intermediate certificate is issued by the certificate preceding it in the chain.

To use chained certificates in your deployment, you must install the appropriate client-side certificates in each user's Web browser and then upload the corresponding CA certificates to Pulse Client Service Intermediate CA store. Use one of the following methods to upload the certificate chain:

1. Import the entire certificate chain in one file. The file must contain the root certificate and any subcertificates whose parents are in the file or already imported. You can include certificates in any order in the import file.
2. Import the certificates one at a time in descending order. You must install the root certificate first, and then install the remaining chained certificates in descending order.

If you follow one of these methods, the system automatically chains the certificates together in the correct order and displays them hierarchically in the admin console.

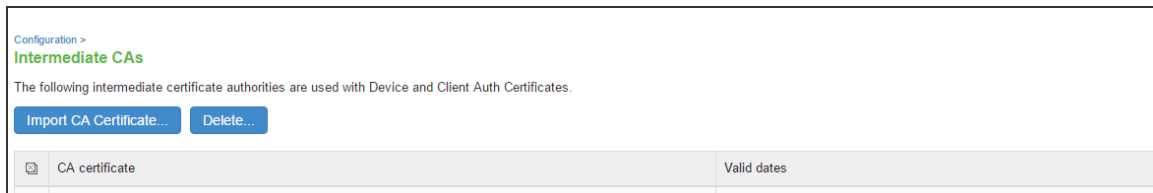


If you install multiple certificates in a user's Web browser, the browser prompts the user to choose which certificate to use when signing in.

Importing Intermediate CA Certificates

To import an intermediate CA certificate:

1. Select **System > Configuration > Certificates > Device Certificates**.
2. Click the **Intermediate Device CAs** link to display the management page.
3. Click **Import CA certificate**
4. Browse to the certificate file, select it, and click **Import Certificate** to complete the import operation.



Importing a Renewed Certificate That Uses the Existing Private Key

You can renew a device certificate in two ways:

- **Submit a new CSR to a CA**—This process is more secure because the CA generates a new certificate and private key and retires the older private key. To use this renewal method, you must first create a CSR through the admin console.
- **Request renewal based on the CSR previously submitted to the CA**—This process is less secure, because the CA generates a certificate that uses the existing private key.

When you order a renewed certificate, you must either resubmit your original CSR or ensure that the CA has a record of the CSR that you submitted for your current certificate.

To import a renewed device certificate that uses the existing private key:

Follow your CA's instructions for renewing a certificate that you previously purchased through them. Be sure to specify the same information you used in the original CSR. Your CA uses this information to create a new certificate that corresponds to the existing key.



Even though you specify the same information used in the original CSR, your root CA might have different serial numbers and keys from the original. You might need to support both new client and old client certificates during the transition period, which also requires that you maintain two root CA certificates (your existing certificate and the renewed certificate), at least temporarily

1. Select **System > Configuration > Certificates > Device Certificates**.
2. Click the link that corresponds to the certificate you want to renew.
3. Click **Renew Certificate** to display the page.
4. In the Renew the Certificate form, browse to the renewed certificate file, enter the password for the certificate key, and click **Import**.

The screenshot shows a web interface for renewing a certificate. At the top, there is a breadcrumb trail: Configuration > Certificates > Renew Certificate. Below this, the title 'Renew Certificate' is displayed in green. A note states: 'Use the form below to renew an existing certificate. If the file is encrypted, you will also need to specify the password.' The form contains two fields: 'Certificate File:' with a blue 'Browse' button and the text 'No file chosen', and 'Password Key:' with an empty text input field. At the bottom of the form is a blue 'Import' button.

Downloading a Device Certificate

You download the device certificate to your local host so that you can import it into other network devices as needed.

To download a device certificate:

1. Select **System > Configuration > Certificates > Device Certificates**.
2. Click the link of the device certificate you want to download to display the configuration page.
3. Click the **Download** link.
4. Save the file to the desired location.

Using Device Certificates with Virtual Ports

Virtual ports can be used to create multiple fully qualified domain names for user sign-in.

When a user tries to sign in using the IP address defined in a virtual port, the system uses the certificate associated with the virtual port to initiate the SSL transaction and for NetScreen Address Change Notification (NACN) communications with the Infranet Enforcer.

You must associate the signed certificate with the port that is connected to the Infranet Enforcer. You can use the same port and certificate for Pulse Client.

You can implement digital certificate security with virtual ports in either of the following ways:

- **Associate all hostnames with a single certificate**—With this method, you use a single wildcard certificate to validate the identity of all system hostnames, regardless of which hostname is used to sign into. A wildcard certificate includes a variable element in the domain name, making it possible for users who sign in from multiple hosts to map to the “same” domain. For example, if you create a wildcard certificate for *.yourcompany.com, the system uses the same certificate to validate its identity to users who sign in to employees.yourcompany.com as it does to users who sign into partners.yourcompany.com.

- **Associate each hostname with its own certificate**—With this method, you associate different hostnames with different certificates. Create a virtual port for each hostname. A virtual port activates an IP alias on a physical port. For example, you can create two virtual ports on a single appliance, mapping the first virtual port to the IP address 10.10.10.1 (sales.yourcompany.com) and the second virtual port to the IP address 10.10.10.2 (partners.yourcompany.com). Then you can associate each of these virtual ports with its own certificate, ensuring that users authenticate through different certificates.

To associate certificates with virtual ports:

- Create the virtual ports.
- Import the device certificates.
- Associate the device certificates with the virtual ports:
 1. Select **System > Configuration > Certificates > Device Certificates**.
 2. Click the link of the device certificate you want to configure to display the configuration page.
 3. Use the controls in the “Present certificate on these ports” section to associate ports with the certificate.



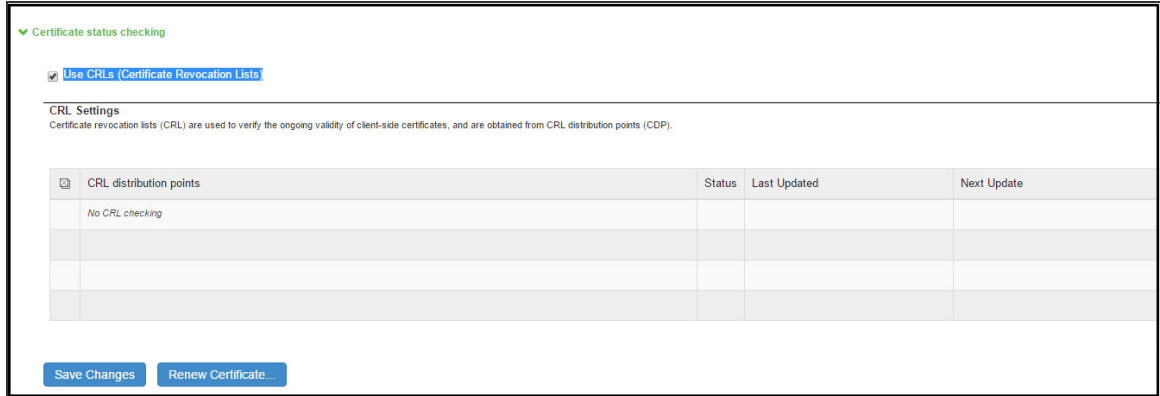
You can assign only one device certificate to the Management Port. If you assign a certificate other than the default device certificate to the Management Port, the default device certificate is automatically deselected as the default. If you do not select a device certificate for the Management Port, the system uses the default device certificate that is presented on the Internal port. You cannot assign certificates to Management Port VIPs.

Enabling Certificate Revocation Check for Device Certificate

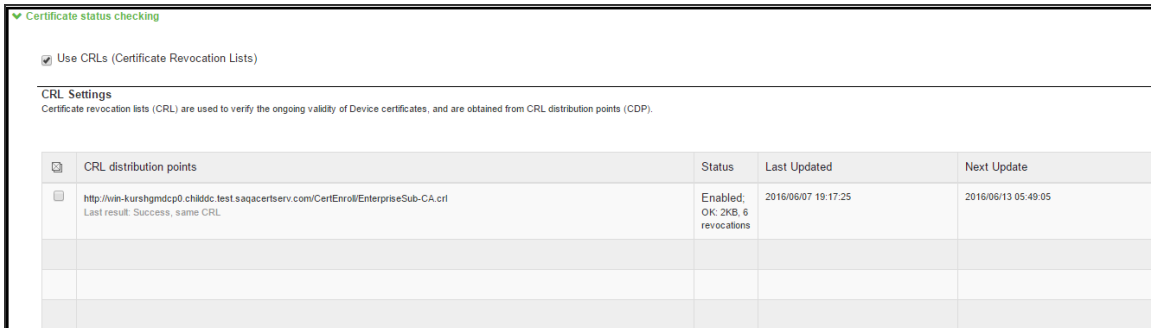
To enable the CRL for Device Certificates:

1. Go to **System > Configuration > Certificates > Device Certificates**.
2. Click on the certificate from the list to go to the certificate details.

- In the Certificate Details page, go to **Certificate Status Checking** and enable the **Use CRLs (Certificate Revocation Lists)** checkbox.



- Click on **Save Changes**.
- Import the CA or CA Chain that issued the Device Certificate to System > Configuration > Trusted Server CAs. Once the CRL is successfully downloaded for Device Certificate, it is listed in the CRL distribution points.



i Ivanti Policy Secure(IPS) supports 3072-bit key length for Device Certificates.

Configuration > Certificates > New Certificate Signing Request

New Certificate Signing Request

Use this page to create a new Certificate Signing Request (CSR) to send to your Certificate Authority of choice.

Common Name:
(e.g., secure.company.com)

Organization Name:
(e.g., Company Inc.)

Org. Unit Name:
(e.g., IT Group)

Locality:
(e.g., SomeCity)

State (fully spelled out):
(e.g., California)

Country (2 letter code):
(i.e., US)

Email Address:

Key Type:
 RSA ECC

Key Length:
1024 bits
1024
2048
3072

Please enter some random characters in the box provided by the system's random key generator. We recommend that you enter approximately twenty characters.

Random Data:
(used for key generation)

Using Trusted Client CAs

This topic describes how to use trusted client Certificate Authorities (CAs).

Understanding Trusted Client CAs

A trusted client CA is a CA that you deem trusted by adding it to the trusted client CA store. The system trusts any certificate issued by that CA. To use client CA certificates, you must install and enable the proper certificates. Additionally, you must install the corresponding client-side certificates in your users' Web browsers, or you must use the MMC snap-in in your users' computer accounts (machine certificate). When validating a client-side CA certificate, the system verifies that the certificate is not expired or corrupt and that the certificate is signed by a CA that the system has been configured to recognize. If the CA certificate is chained, the system also follows the chain of issuers until it reaches the root CA, validating each issuer in turn. The system supports X.509 CA certificates in DER and PEM encode formats.

When you install a client-side certificate, you must determine whether to use the certificate to identify individual users or individual machines. To use the certificate to identify individual users, you must install the certificate in each user's individual certificate store. Then you must enable authentication using a certificate server, or you must enable authorization using realm, role, and/or resource policy settings. To use the certificate to identify individual machines, you must install the certificate in each computer's certificate store. Then you must configure a Host Checker policy that checks for the machine certificate and authorizes access to realms, roles, or resource policies based on the certificate's validity.

The system supports using the following additional features with CA certificates:

- **Certificate servers**—A certificate server is a type of local authentication server that allows you to authenticate users based solely on their certificate attributes rather than authenticating them against a standard authentication server (such as LDAP or RADIUS), and it requires specific certificates or certificate attributes.
- **Certificate hierarchies**—Within a certificate hierarchy, one or more subordinate certificates (called intermediate certificates) are branched off a root certificate to create a certificate chain. Each intermediate certificate (also called a chained certificate) handles requests for a part of the root CA domain. For example, you can create a root certificate that handles all requests to the yourcompany.com domain and then branch off intermediate certificates that handle requests to partners.yourcompany.com and employees.yourcompany.com. When you install a chained certificate, the system confirms that the chain is valid and allows users to authenticate using the leaf certificate (that is, the lowest certificate in the chain).
- **Certificate revocation lists**—Certificate revocation is a mechanism by which a CA invalidates a certificate before its expiration date. The CA publishes a certificate revocation list (CRL) which is a list of revoked certificates. Within CRLs, each entry contains the serial number of the revoked certificate, the date that the certificate was revoked, and the reason the certificate was revoked. The CA can invalidate a certificate for various reasons such as when the employee to whom the certificate is issued leaves the company, the certificate's private key is compromised, or the client-side certificate is lost or stolen. When the CA revokes a certificate, the system can appropriately deny access to users who present a revoked certificate.

Trusted Client CA Implementation Notes

Uploading a trusted client CA certificate does not enable client-side SSL authentication or authorization. To do so, you must use a certificate server, or enable certificate restrictions at the realm, role, or resource policy level, or create a Host Checker policy that verifies a machine certificate.

With client-side certificates, we strongly recommend that you advise users to close their Web browsers after signing out. If they do not, other users might be able to use their open browser sessions to access certificate-protected resources without reauthentication. After loading a client-side certificate, Internet Explorer caches the certificate's credentials and private key. The browser keeps this information cached until the user closes the browser (or, in some cases, until the user reboots the workstation). For details, see <http://support.microsoft.com/?kbid=290345>.) To remind users to close their browsers, you can modify the sign out message on the Sign-in Pages tab.



Certificate authentication does not work on Internet Explorer 8 and 9 if SSL 2.0 is enabled with other SSL and TLS versions. For details, see <http://support.microsoft.com/kb/2851628>.

Understanding CRLs

A certificate revocation list (CRL) is a mechanism for canceling a client-side certificate. As the name implies, a CRL is a list of revoked certificates published by a CA or a delegated CRL issuer. The system supports base CRLs, which includes the company's revoked certificates in a single, unified list.

The system determines the correct CRL to use by checking the client's certificate. (When it issues a certificate, the CA includes CRL information for the certificate in the certificate itself.) To ensure that it receives the most up-to-date CRL information, the system periodically contacts a CRL distribution point to get an updated list of CRLs. A CRL distribution point (CDP) is a location on an LDAP directory server or Web server where a CA publishes CRLs. The system downloads CRL information from the CDP at the interval specified in the CRL, at the interval that you specify during CRL configuration, and when you manually download the CRL. The system also supports CRL partitioning. CRL partitioning enables you to verify portions of very large CRLs without spending the time and bandwidth necessary to access and validate a very large CRL or collection of large CRLs. CRL partitioning is only enabled when you employ the Specify the CDP(s) in the client certificates method (described below). In this case, the system validates the user by verifying only the CRL specified in the client certificate.

Although CAs include CRL information in client-side certificates, they do not always include CDP information as well. A CA can use any of the following methods to notify the system of a certificate's CDP location:

- **Specify the CDP(s) in the CA certificate**—When the CA issues a CA certificate, it might include an attribute specifying the location of the CDPs that the system should contact. If more than one CDP is specified, the system chooses the first one listed in the certificate and then fails over to subsequent CDPs, if necessary.
- **Specify the CDP(s) in the client certificates**—When the CA issues a client-side certificate, it might include an attribute specifying the location of the CDPs that the system must contact. If more than one CDP is specified, it chooses the first one listed in the certificate and then fails over to subsequent CDPs, if necessary. When the system employs CRL partitioning and the client certificate specifies only one CRL, it performs verification using only that CRL.



If you choose this method, the user receives an error on the first sign-in attempt because no CRL information is available. Once the system recognizes the client's certificate and extracts the CRL location, it can start downloading the CRL and subsequently validate the user's certificate. To successfully sign in, the user must try to reconnect after a few seconds.

- Require the administrator to manually enter the CDP location—If the CA does not include the CDP location in the client or CA certificates, you must manually specify how to download the entire CRL object. You can specify a primary and backup CDP. (Manually entering the CDP location provides the greatest flexibility because you do not need to reissue certificates if you change the CDP location.)

The system compares the user's certificate against the appropriate CRL during authentication. If it determines that the user's certificate is valid, the system caches the certificate attributes and applies them, if necessary, during role and resource policy checks. If it determines that the user's certificate is invalid, if it cannot contact the appropriate CRL, or if the CRL is expired, it denies the user access.



- The system supports only CRLs that are in a PEM or DER format and that are signed by the CA for which the revocations apply.
 - The system only saves the first CRL in a PEM file.
-

Understanding OCSP

The Online Certification Status Protocol (OCSP) is a service that enables you to verify client certificates. When OCSP is enabled, the system becomes a client of an OCSP responder and forwards validation requests for users based on client certificates. The OCSP responder maintains a store of CA-published certificate revocation lists (CRLs) and maintains an up-to-date list of valid and invalid client certificates. After the OCSP responder receives a validation request, it validates the status of the certificate using its own authentication database, or it calls upon the OCSP responder that originally issued the certificate to validate the request. After formulating a response, the OCSP responder returns the signed response, and the original certificate is either approved or rejected.

Importing a Trusted Client CA Certificate

If you require users to provide a client-side certificate to sign in, you must upload the corresponding CA certificate. You can upload CA certificates manually, or you can configure the system to upload CA certificates automatically. The system uses the uploaded certificate to verify that the browser-submitted certificate is valid. In addition, you can specify if you want to automatically import CA certificates for validation, and you can specify a CRL or OCSP retrieval method to use to automatically import CA certificates.

To import a trusted client CA certificate:

1. Select **System > Configuration > Certificates > Trusted Client CAs** to display the configuration page.
2. Click **Import CA Certificate** to display the configuration page.
3. Browse to the certificate file, select it, and click **Import Certificate** to complete the import operation.

Renewing a Certificate

To renew a certificate:

1. Select **System > Configuration > Certificates > Trusted Client CAs**.
2. Click the link for the certificate you want to renew.
3. Click **Renew Certificate** to display the import certificate page.
4. Browse to the certificate file, select it, and click **Import Certificate** to complete the import operation.

Configuring Auto-Importing of Client Certificates

To enable auto-importing:

1. Select **System > Configuration > Certificates > Trusted Client CAs**.
2. Click the **Auto-Import Options** button to display the options.
3. Complete the configuration described in table.
4. Save your changes.

Settings	Guidelines
Auto-import trusted CAs	Select this option to enable auto-import and display its configuration settings.
Client Certificate Status Checking	Select a method to validate the trusted client certificate: <ul style="list-style-type: none"> • None—Do not validate.

Settings	Guidelines
	<ul style="list-style-type: none"> • Use OCSP—Use the OCSP method, validating the client certificate in real-time, as needed. After you select this option, you can specify options for OCSP. • Use CRLs—Use CRLs to validate the client certificate. After you select this option, you can specify options for OCSP. • Use OCSP with CRL fallback—Use the OCSP validation method when possible, but attempt to validate client certificates using CRLs if the OCSP method fails (for example, if the link to the OCSP responder fails). After you select this option, you can specify options for OCSP. • Inherit from root CA—Use the method configured for the device certificate.
CDP(s)/OCSP responder	<p>Select the location of the responder value:</p> <ul style="list-style-type: none"> • None—Do not use the responder. • From client certificate—Use the responder value configured in the client certificate. • From trusted CA certificate—Use the responder value configured in the trusted CA certificate that has been uploaded to the system.
Verify imported CA certificates	<p>Select this option to verify that this trusted client CA is valid. Enabling this will check the CRL of this certificate's issuer, and repeat up the chain until reaching the root trusted client CA.</p>
Skip Revocation check when OCSP/CDP server is not available	<p>Select this option to instruct IPS to skip revocation check and accept end user certificates when either OCSP server or CDP server is not accessible over the network. This option is applicable to digital certificates used for end user authentication.</p> <p>IPS skips the revocation check in the following conditions:</p> <ul style="list-style-type: none"> • Server IP is not reachable • Server Hostname is either not resolvable or resolving to non OCSP/CRL Server IP • Proxy IP is either not reachable or not resolving

Settings	Guidelines
	<ul style="list-style-type: none"> • Download CRL has expired • OCSP/CRL service in Server is not responding

Configuring Options for Trusted Client CA Certificates

To configure options for the trusted client CA certificate:

1. Select **System > Configuration > Certificates > Trusted Client CAs**.
2. Under **Port Selection for CRL and OCSP Download**, select the port: Internal Port, External Port, or Management Port.

Configuration > Certificates > Trusted Client CAs

Trusted Client CAs

Configuration Certificates

Licensing Pulse One Security Certificates DMI Agent Sensors Client Types Guest Access Notification

Device Certificates Trusted Client CAs Trusted Server CAs Client Auth Certificates Certificates Validity Check

Port Selection for OCSP and CRL Traffic

Internal Port
 External Port
 Management Port

Note: Port Selection settings are node-specific. Please configure the settings individually for different nodes in cluster

Save

Users can be required to present valid client-side certificates to sign in(see the realm-specific Certificate Authentication Policy page). Specify trusted certificate authorities.

Auto-import options... Proxy Settings... Import CA Certificate... Delete...

10 records per page Search:

Trusted Client CA	Trusted for client authentication?	Valid dates	Status checking
[icon] [name]	Yes	2018/07/31 - 2028/07/31	None

3. Click the certificate you want to configure.

4. Complete the configuration described in the following table.

Settings	Guidelines
Certificate	<p>Use the expander buttons to display the following details:</p> <ul style="list-style-type: none"> • Issued To—Name and attributes of the entity to whom the certificate is issued. • Issued By—Name and attributes of the entity that issued the certificate. Note that the value of this field must match either the Issued To field (for root certificates) or the Issued To field of the next highest certificate in the chain (for intermediate certificates). • Valid Dates—Time range for which the certificate is valid. • Details—Various certificate details, including its version, serial number, signature algorithm, CRL distribution points, public key algorithm type, and public key.
Client Certificate Status Checking	<p>Select a method to validate the trusted client certificate:</p> <ul style="list-style-type: none"> • None—Do not validate. • Use OCSP—Use the OCSP method, validating the client certificate in real-time, as needed. After you have selected this option and saved the configuration, you can specify options for OCSP. • Use CRLs—Use CRLs to validate the client certificate. After you have selected this option and saved the configuration, you can specify options for CRL. • Use OCSP with CRL fallback—Use the OCSP validation method when possible, but attempt to validate client certificates using CRLs if the OCSP method fails (for example, if the link to the OCSP responder fails). After you have selected this option and saved the configuration, can specify options for OCSP and CRL.

Settings	Guidelines
Verify Trusted Client CA	Select this option to verify that this trusted client CA is valid. Enabling this will check the CRL of this certificate's issuer, and repeat up the chain until reaching the root trusted client CA.
Trusted for Client Authentication	Clear this check box to exclude the CA from being trusted for client certificate authentication. You might want to do this if this CA was added for another trusting purpose, such as SAML signature verification or machine certificate validation.
Skip Revocation check when OCSP/CDP server is not available	<p>Select this option to instruct IPS to skip revocation check and accept end user certificates when either OCSP server or CDP server is not accessible over the network. This option is applicable to digital certificates used for end user authentication.</p> <p>IPS skips the revocation check in the following conditions:</p> <ul style="list-style-type: none"> • Server IP is not reachable • Server Hostname is either not resolvable or resolving to non OCSP/CRL Server IP • Proxy IP is either not reachable or not resolving • Download CRL has expired • OCSP/CRL service in Server is not responding

5. Save your changes.
6. If you have enabled CRL Checking, click **CRL Checking Options**.

7. If you have enabled OCSP options:

- Click **OCSP** Options.
- Complete the configuration described in the following table.

Settings	Guidelines
Use	<p>Select the type of OCSP responder to validate trusted client CAs:</p> <p>None—The system does not use OCSP to verify the status of certificates issued by this CA.</p> <p>Responder(s) specified in the CA certificate—The system uses OCSP responders specified in the imported client CA to perform verification. When you select this option, the system displays a list of OCSP responders specified in the imported CA (if any) and the last time they were used.</p> <p>Responder(s) specified in the client certificates—The system uses responders specified during client authentication to perform verification. When you select this option, the system displays a list of known OCSP responders (if any) and the last time they were used.</p> <p>Manually configured responders—The system uses primary and secondary OCSP responders at the addresses you specify.</p>
Device Certificate to sign the request	Select the appropriate device certificate or leave the default (unsigned).
Signature Hash Algorithm	Select SHA-1 or SHA-2.
Use Nonce	A nonce is random data the system includes in an OCSP request and the OCSP responder returns in the OCSP response. The system compares the nonce in the request and response to ensure that the response is generated by the OCSP responder. If the two do not match, the system disregards the response and sends a new request.

8. Save the configuration.

9. After you have added an OCSP responder to the list, you can click its link to display the page.

10. Complete the configuration described in the following table.

Settings	Guidelines
Responder Signer Certificate	Browse to the network path or local directory location of a Responder Signer Certificate. This is the certificate the OCSP responder uses to sign the response. You must specify the Responder Signer Certificate if the signer certificate is not included in the response.
Trust Responder Certificate	Select this option to allow an OCSP responder certificate that matches the responder signer certificate.
Revocation Checking	Select this option to ensure that the certificate has not recently been revoked. This option has implications only if you specified the Use OCSP with CRL fallback option.
Allow clock discrepancy	Use this option to account for possible mismatches in timestamps between the system clock and the OCSP responder clock. If the mismatch is significant, the system disregards the response from the OCSP responder as out of date or expired.

11. Save the configuration.

Configuring a Proxy Server for CRL Downloads and OCSP Status Checks

You can configure the system to send CRL download requests and OCSP status checks to the proxy server and collect the response. You might want to do this if you deploy proxy server to control access to the Internet.


The following types of CRL downloads can use the proxy server:

- CRL distribution points (CDPs) specified in the trusted client CAs
- CDPs specified in client certificates
- Manually configured CDPs

Similarly, the system can send OCSP requests to the OCSP responder through the proxy server. The OCSP responses are also received through the proxy server. This feature is useful when you deploy many IPS systems and the OCSP responders are located outside the network.

To configure a proxy server:

1. Select **System > Configuration > Certificates > Trusted Client CAs**.
2. Click **Proxy Settings** to display the page.
3. Complete the configuration described in the following table.
4. Save the configuration.

Settings	Guidelines
Use Proxy Server for HTTP-based CRL download	<p>Select to enable the CRL operations to use a proxy server.</p> <p> You can configure a proxy server for web-based URLs, not LDAP URLs.</p>
Use Proxy Server for HTTP-based OCSP status checking	Select to enable the OCSP operations to use a proxy server.
Host Address	Specify either an IP address or a fully qualified domain name.
Port	Enter the proxy server port number if it is different from the default value of 80.
Username/password	If your proxy server required authentication, enter a username and password to log in to the proxy server.

Using Client Auth Certificates

This topic describes how to use client auth certificates.

Understanding Client Auth Certificates

In certain corporate environments, servers on the LAN are protected with two-way SSL authentication. These servers require the client to authenticate by presenting a valid certificate.

In the remote access scenario, ICS is a client of these servers. You can configure IPS to present client authentication certificates to servers whenever it communicates over SSL.

 This feature authenticates end users or end-user machines to servers on the corporate LAN.

The SSL protocol provides for mutual authentication of server and client at the time of session initiation. The client part of the authentication is optional. For enhanced security, some deployments may require that the client also authenticate itself with a certificate. Normally, when setting up an SSL connection with a server on behalf of the end user, ICS does not present any certificate to the server. It needs to be explicitly configured to present such certificate. This section explains how such configuration may be performed.

The basic idea is to upload a certificate, private key pair to the Pulse Secure access management framework, and configure a mapping between this pair and a server resource. Subsequently, when an end user attempts to establish a connection with that server, IPS presents the associated certificate to the server. If no certificate is associated with the server in ICS certificate store, then it is assumed that the server does not demand client certificate.

If, during the SSL handshake, the back-end server requests a client certificate but IPS doesn't send a certificate, the end user sees an "access denied" error message. Similarly, if the back-end server rejects the IPS certificate, the end user sees an "access denied" error message. If a certificate is configured, is successfully retrieved and no error is encountered during handshake, the user is granted access to the server.



The IPS access management framework allows client authentication certificates to be uploaded to the device in two ways: generate a CSR and upload the signed certificate returned by the CA, or directly import the certificate if one is available.

Importing a Client Auth Certificate

The Pulse Secure access management framework allows certificates that include the private key and for instances where the private key is in a separate file from the certificate. In addition, if your certificates have been exported into a system configuration file, you can import the system configuration file to upload the certificates.

To import the client auth certificates files:

1. Select **System > Configuration > Certificates > Client Auth Certificates**.
2. Click **Import Certificate & Key** to display the configuration page.
3. Complete the configuration described in table.
4. Click **Import**.

Settings	Guidelines
If certificate file includes private key	
Certificate File	Browse to the network path or local directory location of your private key file.
Password Key	Enter the password key.
If certificate and private file are separate keys	
Certificate File	Browse to the network path or local directory location of your certificate key file.
Private Key File	Browse to the network path or local directory location of your private key file.
Password Key	Enter the password key.
Import via System Configuration file	
System Configuration File	Browse to the network path or local directory location of the system configuration file.
Password	Enter the password.

Renewing a Client Auth Certificate

To renew a certificate:

1. Select **System > Configuration > Certificates > Client Auth Certificates**.
2. Click the link that corresponds to the certificate you want to renew.
3. Click **Renew Certificate** to display the configuration page.
4. In the **Renew the Certificate** form, browse to the renewed certificate file, enter the password for the certificate key, and click **Import**.

Configuring Two-Way SSL Authentication

To configure two-way SSL authentication:

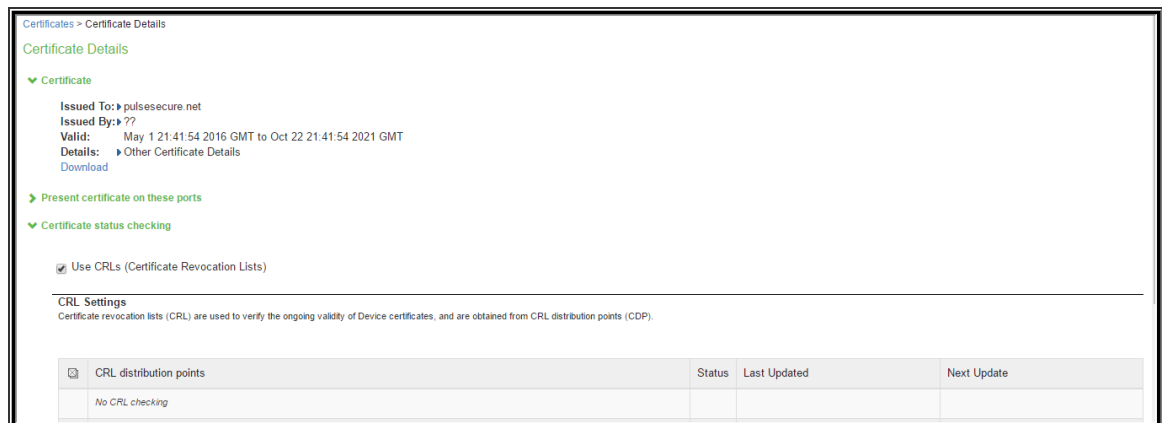
1. Import the certificates used for two-way SSL handshake in the **System > Configuration > Certificates > Client Auth Certificates** window.
2. Define the back-end resource and assign a certificate to be presented when accessing it using the **Users > Resource Policies > Web > Client Authentication** window.

Enabling Certificate Revocation Check for Client Auth Certificate

Client Auth Certificate Revocation Check is only applicable for TLS Syslog Backend Server. It is not applicable for any other backend server configured to ask Client Certificate.

To enable the CRL for Client Auth Certificate:

1. Go to **System > Configuration > Certificates > Client Auth Certificates**.
2. Click on the certificate from the list to go to the certificate details.
3. In the Certificate Details page, go to **Certificate Status Checking** and enable the Use CRLs (Certificate Revocation Lists) (Certificate Revocation Lists) checkbox.



4. Click on **Save Changes**.
5. Import the CA or CA Chain that issued the Client Auth Certificate to **System > Configuration > Trusted Client CAs**.
6. Once the CRL is successfully downloaded for Client Auth Certificate, it is listed in the CRL distribution points.

Certificate Status Checking

Use CRLs (Certificate Revocation Lists)
Note: This option only applies to the Syslog Server.

CRL Settings
Certificate revocation lists (CRL) are used to verify the ongoing validity of Client Authentication certificates, and are obtained from CRL distribution points (CDP).

CRL distribution points	Status	Last Updated	Next Update
<input type="checkbox"/> http://win-kurshgndcp0.chiddc.test.saaqcertserv.com/CertEnroll/EnterpriseSub-CA.crl <small>Last result: Success, same CRL.</small>	Enabled; OK: 2KB, 6 revocations	2016/06/08 13:19:57	2016/06/13 05:49:05



This version of the IPS supports the 3072 bit key length for Client Auth Certificates.

Configuration > Certificates > New Certificate Signing Request

New Certificate Signing Request

Use this page to create a new Certificate Signing Request (CSR) to send to your Certificate Authority of choice.

Common Name:
(e.g., secure.company.com)

Organization Name:
(e.g., Company Inc.)

Org. Unit Name:
(e.g., IT Group)

Locality:
(e.g., SomeCity)

State (fully spelled out):
(e.g., California)

Country (2 letter code):
(i.e., US)

Email Address:

Key Type:
 RSA ECC

Key Length: bits

Please enter some random characters in the Random Data field using the system's random key generator.
We recommend that you enter approximately twenty characters.

Random Data:
(used for key generation)



CRL Download for Device Certificate and Client Auth Certificate using LDAP based URL won't work due to dependency of LDAP Username and Password. In some cases, CDP LDAP URL hostname field is also required which is also not supported.

Using Trusted Server CAs

This topic describes trusted server certificate authorities (CAs).

Understanding Trusted Server CAs

All the trusted root CAs for the Web certificates installed in Internet Explorer are preinstalled. You might need to install a trusted server CA for additional Web servers in the following situations:

- If you are using third-party integrity measurement verifiers (IMVs) that are installed on a remote server, you must upload the trusted root certificate of the CA that signed the remote server's server certificate.
- If you are using virus signature version monitoring with your own staging site for storing the current virus signatures list, you must upload the trusted root certificate of the CA that signed the staging server certificate.
- You can install the trusted root CA certificate on the endpoint in any of the following ways:
- Use a CA certificate that is chained to a root certificate that is already installed on the endpoint, such as VeriSign.
- Upload the CA certificate and any intermediate CA certificates to the Pulse Client system. During client installation, the system automatically installs the trusted root device CA certificates on the endpoint. When prompted during installation, the user must allow the installation of the CA certificate(s).
- Prompt users to import the CA certificates on the endpoint using Internet Explorer or other Microsoft Windows tools. In other words, you can use common methods organizations use to distribute root certificates.



You cannot use CRL revocation checks for trusted server CA certificates.

Uploading Trusted Server CA Certificates

You can use the Trusted Server CAs page to upload the trusted root certificate of the CA that signed the Pulse Client service device certificate. If you upload a certificate chain, you must install the certificates one at a time in descending order starting with the root certificate (DER or PEM files), or you must upload a single file that contains the entire certificate chain (PEM files only). The system supports X.509 CA certificates in PEM (Base 64) and DER (binary) encode formats.

To upload CA certificates:

1. Select **System > Configuration > Certificates > Trusted Server CAs** to display the page.
2. Click **Import Trusted Server CA** to display the page.
3. Browse to the certificate file, select it, and click **Import Certificate** to complete the import operation.

Restoring the Prepopulated Group of Trusted Server CA Certificates

The System > Configuration > Certificates > Trusted Server CAs page is prepopulated with some of the trusted root CAs for the Web certificates installed in Internet Explorer and Windows. You can use the delete functionality on this page to delete CAs and the reset functionality to restore the list to the set that was installed during the upgrade. The reset operation clears all manually imported certificates.

To restore the prepopulated group of trusted CA certificates:

1. Select **System > Configuration > Certificates > Trusted Server CAs**.
2. Click **Reset Trusted Server CAs**.
3. Confirm that you want to restore the set of trusted server CAs that was installed when you upgraded.

Renewing a Trusted Server CA Certificate

If a trusted CA renews its certificate, you must upload the renewed CA certificate.

To import a renewed CA certificate:

1. Select **System > Configuration > Certificates > Trusted Server CAs**.
2. Click the link that corresponds to the certificate that you want to renew to display the page.
3. Click **Renew Certificate**.
4. Browse to the certificate file, select it, and click Import Certificate to complete the import operation.

Deleting a Trusted Server CA Certificate

You can delete any trusted server CA certificate, including preinstalled certificates.

To delete a trusted server CA certificate:

1. Select **System > Configuration > Certificates > Trusted Server CAs**.
2. Select the check box for the certificate you want to delete.
3. Click **Delete**, and then confirm that you want to delete the certificate.

Understanding ECC Certificates

Public-key cryptography is a cryptographic system that requires a secret key and a public key that are mathematically linked with each other. One key encrypts the plain text while the other decrypts the cipher text. RSA is the most widely used public-key algorithm.

Elliptic Curve Cryptography (ECC) were introduced as an alternative to RSA in public key cryptography. One advantage of ECC over RSA is key size versus strength. For example, a security strength of 80 bits can be achieved through an ECC key size of 160 bits, whereas RSA requires a key size of 1024. With a 112-bit strength, the ECC key size is 224 bits and the RSA key size is 2048 bits.

The most popular signature scheme that uses elliptic curves is called the Elliptic Curve Digital Signature Algorithm (ECDSA). The most popular key agreement scheme is called Elliptic Curve Diffie-Hellman (ECDH). An ECDH exchange is a variant of the Diffie-Hellman (DH) protocol and is an integral part of the Suite B cryptography standards proposed by the National Security Agency (NSA) for protecting both classified and unclassified information.

About Suite B

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. Because a single encryption algorithm cannot satisfy all the needs of the national security community, NSA created a larger set of cryptographic algorithms, called Suite B, which can be used along with AES in systems used by national security users. In addition to AES, Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchanges.

Per RFC 6460, to be Suite B TLS 1.2 compliant the server and client should negotiate with the following ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

RFC 6460 also lists a transitional Suite B profile for TLS 1.0 and TLS 1.1. Clients and servers that do not yet support Suite B TLS 1.2 should negotiate with the following ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

There is no special configuration to ensure that IPS negotiates Suite B ciphers. However, the following general steps should be performed to enable Suite B compliance:

- An ECC certificate signed by an ECC Root CA is associated with a network port.
- A P-256 CSR is signed by either a P-256 or P-384 Root CA.
- A P-384 CSR is signed by a P-384 Root CA.
- Manually enable only AES128 and/or AES256 custom ciphers.



IPS cannot be configured to allow only Suite B ciphers.

Using ECC Certificates

ECC certificates are currently supported only on the virtual appliance platforms. As with RSA certificates, ECC certificates are associated with a network port. You can create multiple virtual ports on the server with each port supporting a specific certificate. For example, external virtual port 1 can use a 1024-bit RSA while external virtual port 2 uses ECC P-256 and external virtual port 3 uses ECC P-384. Only clients that support ECC cipher suites can connect to the web server on that network port.

When an Elliptic Curve Cryptography (ECC) certificate is associated with a network port, only clients that support ECC cipher suites can connect to the Web server on that network port.

Except for the key and certificate generation process, the use of ECC certificates is basically the same as using RSA certificates.

File Management

Overview

The system supports multiple administrator capabilities related to configuration and log file management.

The below list describes the purpose of the different features:

- Archiving- This feature helps to archive system and user configuration files and user logs on a remote backup server. It also helps in scheduling the archiving jobs. The system allows to import the configurations archived.
- Local backup and restore- This feature helps to create backups on the local system and then recover or restore the data during a disaster or while doing significant configuration changes.
- Binary configuration file import/export- This feature helps to export or import the system (system.cfg) and user configuration (user.cfg) in a binary format to replicate the configuration across multiple systems and across the system upgrades.
- XML configuration file import/export- This feature helps to selectively or fully import or export the configuration in an XML format from one IPS device to another. The XML configurations can be modified for system details such as IP address and so on before importing.
- Push Configuration- This feature helps to push a partial configuration from one IPS device to one or more IPS devices directly.

Configuration

The Admin can perform the following configuration procedures:

Archiving

The Admin must configure the archiving backup server details to transfer the files. You can also schedule the archiving jobs.



- The system does not continue to retry the process if it fails, and log files are not deleted.
- It is recommended to schedule an archive operation when traffic is low to minimize its impact on users. The automatic archiving process compresses files and may lead to performance issues.
- The daylight savings time (DST) must be considered while scheduling the archiving.

To configure log archiving:

1. Select **Maintenance > Archiving > Archiving Servers** to display the configuration page.
2. Complete the configuration as described in table.
3. Save the configuration.

The screenshot shows the 'Archiving Servers' configuration page. It includes a 'Save Changes' button at the bottom left. The 'Archive Settings' section has radio buttons for Method (SCP, FTP, AWS S3, Azure Storage) and input fields for Archive Server, Destination Directory, Username, and Password. The 'Archive Schedule' section has checkboxes for various log types: Archive events log, Archive user access log, Archive admin access log, Archive Sensors log, Archive system configuration, Archive user accounts, Archive XML configuration, Archive Debug Log, and Archive Periodic SnapShots.

Settings	Guidelines
Archive Settings	
Archive Server	Specify the fully qualified domain name or IPv4/IPv6 address of the server to which to send the archive files.
Destination Directory	Specify the destination directory. Follow these recommendations:

Settings	Guidelines
	<p>For UNIX systems, you can specify an absolute or relative path. We recommend you specify a full path.</p> <p>For Windows systems, specify a path that is relative to the ftp root directory. We recommend you specify a full path.</p>
	<p>Do not include a drive specification for the destination directory, such as: pulsesecure/log.</p>
Username	<p>Specify a username that has privileges to log into the server and write to the destination directory.</p>
Password	<p>Specify the corresponding password.</p>
Method	<p>Select SCP, FTP, AWS S3 or Azure Storage.</p> <p>SCP is the default method. SCP is a file transfer utility similar to FTP. SCP encrypts all data during transfer. When the data reaches its destination, it is rendered in its original format. SCP is included in most SSH distributions and is available on all major operating system platforms.</p> <p>AWS S3: Push backup configurations and archived logs to Amazon AWS S3 bucket. For more details, refer to <i>Ivanti Connect Secure Virtual Appliance on Amazon AWS Cloud Deployment Guide</i>.</p> <p>Azure Storage: Push backup configurations and archived logs to Microsoft Azure storage. For more details, refer to <i>Ivanti Connect Secure Virtual Appliance on Microsoft Azure Cloud Deployment Guide</i>.</p>
Archive Schedule	

Settings	Guidelines
Archive events log	<p>Schedule archiving for the Events log. The archive file has the following format: PulseSecureEventsLog-[clustername standalone]-[nodename hostname]-[date]-[time]</p> <p>For example, an archive file for a cluster named Gen has a filename similar to the following: PulseSecureEventsLog-Gen-node1-Root-20090109-1545.gz.</p> <p>The archiving schedule configuration includes the following options:</p> <ul style="list-style-type: none"> • Use this filter-Select a log format filter. • Day of week-Select the days of the week on which to run the archiving job. • Every hour or a Specified Time. Every hour option runs a job every hour on the hour for the selected days. The specified time option runs a job once on the selected days. • Clear log after archiving. Select this option to clear the local log file after the archiving job is successfully completed. If an archive job fails, the log files are not deleted.
Archive user access log	<p>Schedule archiving for the User Access log. The archive file has the following format: PulseSecureAccessLog-[clustername standalone]- [nodename hostname]-[date]-[time]</p> <p>The archiving schedule configuration includes the same options as those described for the Events log.</p>
Archive admin access log	<p>Schedule archiving for the Admin Access log. The archive file has the following format: PulseSecureAdminLog-[clustername standalone]- [nodename hostname]-[date]-[time]</p> <p>The archiving schedule configuration includes the same options as those described for the Events log.</p>
Archive sensors log	<p>Schedule archiving for the Sensors log. The archive file has the following format: PulseSecureSensorsLog-[clustername standalone]- [nodename hostname]-[date]-[time]</p> <p>The archiving schedule configuration includes the same options as those described for the Events log.</p>

Settings	Guidelines
Archive system configuration	<p>Schedule archiving for the system configuration binary file (system.cfg). The archive file has the following format:</p> <p>PulseSecureConf-[clustername standalone]- [nodename hostname]-[date]-[time]</p> <p>The archiving schedule configuration includes the same day, time, and password-protection options as those described for the Events log.</p>
Archive user accounts	<p>Schedule archiving for user account configuration binary file (user.cfg). The archive file has the following format:</p> <p>PulseSecureUserAccounts-[clustername standalone]-[nodename hostname]-[date]-[time]</p> <p>The archiving schedule configuration includes the same day, time, and password-protection options as those described for the Events log.</p>
Archive XML configuration	<p>Schedule archiving for the XML configuration files.</p> <p>The archiving schedule configuration includes the same day and time options as those described for the Events log.</p>
Archive debug log	<p>Enable archiving for collected debug logs.</p> <p>You cannot specify a day and time for archiving debug logs. If you select this option, debug logs are archived periodically and cleared if the Clear log after archiving option is selected.</p>
Archive periodic snapshots	<p>Enable archiving for snapshots.</p> <p>You cannot specify a day and time for archiving periodic snapshots. If you select this option, snapshots are archived periodically.</p>

Backup and Restore

Using the backup and restore feature the Administrator can take the system and user account backup and restore it as needed.



System allows you to save five system configuration backups and five user account backups on the local server.

To manage configuration file backups:

1. Select **Maintenance > Archiving > Local Backups** to display the configuration page.
2. Use the controls to backup or restore the configuration as described in the following table.
3. Save the configuration.

Controls	Guidelines
System Configuration	
Save Configuration	Create a backup of the running configuration.
Delete	Select a row in the table and click Delete to delete the backup.
Restore	Select a row in the table and components in the "Include when restoring" column and click Restore to replace the running configuration with the archived configuration.
User Configuration	
Save Configuration	Create a backup of the running configuration.
Delete	Select a row in the table and click Delete to delete the backup.
Restore	Select a row in the table and click Restore to replace the running configuration with the archived configuration.

Importing/Exporting Binary System Configuration Files

Ivanti Policy Secure(IPS) enables you to import and export the system and network settings using binary system configuration files. When importing a system configuration file, you can exclude the device certificate and the server's IP address or network settings from the imported information. For example, to set up multiple IPS systems behind a load balancer, import everything except for the IP address. To set up the system as a backup server, import everything except for the digital certificate and the network settings. The binary system configuration file includes the following settings:

- **Network settings**
 - **Certificates.** The system imports only device certificates, not the chains that correspond to the device certificates or trusted client CAs.
- **Cluster configuration**
 - **Licenses.** When you import a configuration file that contains licenses, the system gives precedence to any existing licenses. Licenses are imported only if no licenses are currently installed.
- **SNMP settings**
 - **Sensor configuration.** Sensor configurations are included in the system configuration file while sensor event policies are included in the user configuration file. To import or export all sensor-related settings, import or export both the system and user configuration files. The user configuration file, not the system configuration file, includes resource profiles, resource policies, and the local user database. To perform a complete backup, export both the system and user configuration files.
 - **Client-side logs.** To import or export client-side logs, import or export both the system and user configuration files.



Import of system and user configuration across different hardware platforms is not supported. You can import a FIPS configuration file into a non-FIPS device and vice versa if you do not include the certificate and security world in the import process.



To export a binary system configuration file:

1. Select **Maintenance > Import/Export > Import/Export Configuration** to display the configuration page.

2. Complete the configuration and import/export operation as described in the following table.

The screenshot shows the 'System Configuration' page with three tabs: 'Configuration', 'User Accounts', and 'XML Import/Export'. The 'Configuration' tab is active. Under the 'Export' section, there are two password input fields labeled 'Password for configuration file:' and 'Confirm Password:', followed by a 'Save Config As...' button. The 'Import' section includes a checkbox for 'Import Device Certificate(s)?' with a note that it will overwrite existing certificates. Below this are radio button options for 'Other Import Options': 'Import everything (except Device Certificate(s))', 'Import everything but the IP address' (with a note about standalone nodes), 'Import everything except network settings, cluster settings and licenses' (with a note about network settings), and 'Import only Device Certificate(s)' (with a note about cluster nodes). There is also a 'Config File:' field with a 'Browse' button and a 'Password:' field with a note to use it for password-protected files. An 'Import Config' button is at the bottom.

Settings	Guidelines
Export	
Password for configuration file	Specify a password to encrypt and secure the configuration file.
Confirm password	Specify the password.
Save Config As	Display a dialog box to save the file to your local host.
Import	
Import Device Certificate(s)?	Overwrite the existing device certificate(s) with the ones in the imported configuration file. NOTE: When importing a device certificate in to a FIPS device, note that you must choose a certificate that uses a FIPS-compliant private key. To ensure FIPS-compliance, select a certificate and corresponding security world private keys were generated on a FIPS device.

Settings	Guidelines
Other Import Options	
Import everything (except Device Certificate(s))	Import all settings except the device certificate.
Import everything but the IP address	<p>Do not overwrite the existing configuration for network interface IP addresses, netmask, default gateway, virtual interfaces, ARP tables, and route tables. Use <u>this option only if the exported configuration file is from a standalone node.</u></p> <p> To set up multiple nodes in a cluster behind a load balancer, import everything except the IP address.</p>
Import everything except network settings and licenses	<p>Do not allow the imported configuration to change the existing configuration for settings found in the Network Settings and Licensing sections. With this option, network configurations, licenses, cluster configurations, certificates, defined SNMP settings and syslog configurations are not imported. Always use this option if configuration file was exported from a node that is part of a cluster.</p> <p> To set up a backup node, import everything except network settings and digital certificates.</p>
Import only Device Certificate (s)	Import the device certificate(s) only.
Config file	Use the browse button to locate and select the file from your local host.
Password	Specify the password (if applicable).
Import Config	Import the configuration file.

Importing/Exporting Binary User Configuration Files

Ivanti Policy Secure(IPS) allows you to import/export the system and network settings using binary configuration files. In general, if a menu item falls under the Authentication, Administration, or Users menu, the item is included in the user configuration file (user.cfg). The exception is Sensors event policies, which are under System, but which are exported in the user configuration file. The user configuration file includes the following settings:

- Sign-in settings (includes sign-in policies, sign-in pages, all authentication servers, authentication protocol sets, Pulse Client settings)
- Authentication realms (including admin realms, user realms, and MAC authentication realms)
- Roles
- Network access.
- Infranet Enforcers.
- Host Enforcer.
- Resource policies
- Sensor event policies
- User accounts
- Client-side logs. To export or import client-side logs, export or import both the system and user configuration files.

To export a binary user configuration file:

1. Select **Maintenance > Import/Export > Import/Export Users** to display the configuration page.

2. Complete the configuration and export/import operation as described in the following table.

The screenshot shows the 'User Configuration' page with three tabs: 'Configuration', 'User Accounts', and 'XML Import/Export'. The 'User Accounts' tab is active. Under the 'Export' section, there are two password input fields labeled 'Password for configuration file:' and 'Confirm Password:', followed by a 'Save Config As...' button. Under the 'Import' section, there is a 'Browse' button, a text input field for a password, and an 'Import Config' button. The text below the 'Import' section reads: 'Import user settings by selecting the configuration file and clicking Import Config. Import User Accounts will invalidate all existing End-User and Administrators sessions.'

Settings	Guidelines
Export	
Password for configuration file	(Optional) Specify a password to encrypt and secure the configuration file.
Confirm password	Specify the password.
Save Config As	Display a dialog box to save the file to your local host.
Import	
Browse	Locate and select the file from your local host.
Password	Specify the password (if applicable).
Import Config	Import the configuration file.

Importing/Exporting XML Configuration Files

The Admin can save the system and user configuration in XML format. This enables the system to replicate the configurations.

This will help in the following use cases:

- Adding to the configurations of peer nodes, for example, adding many users.
- Modifying multiple instances of a single setting, for example, an authentication server name.
- Deleting settings, for example, deleting authentication servers that are no longer used.
- Creating a configuration template to use for setting up new nodes.
- Tracking configuration changes by comparing differences on periodic exports.

Guidelines and Limitations

Table summarizes the guidelines and limitations for using the XML import/export feature.

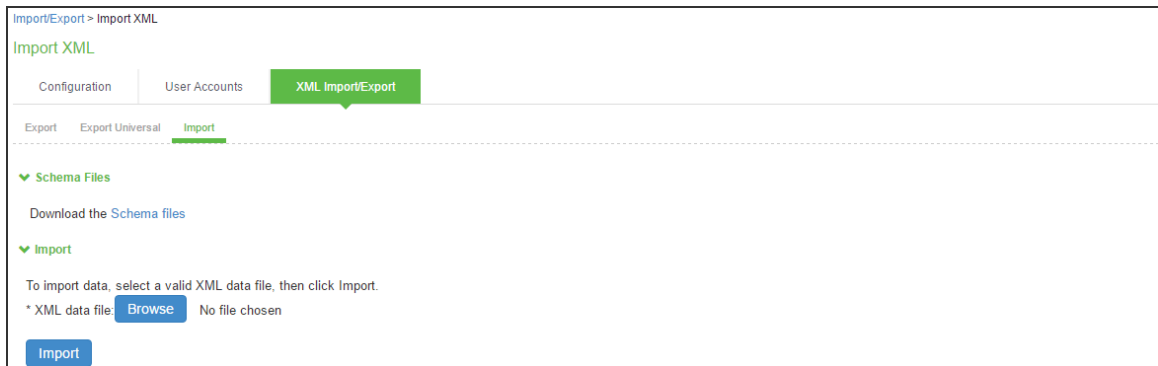
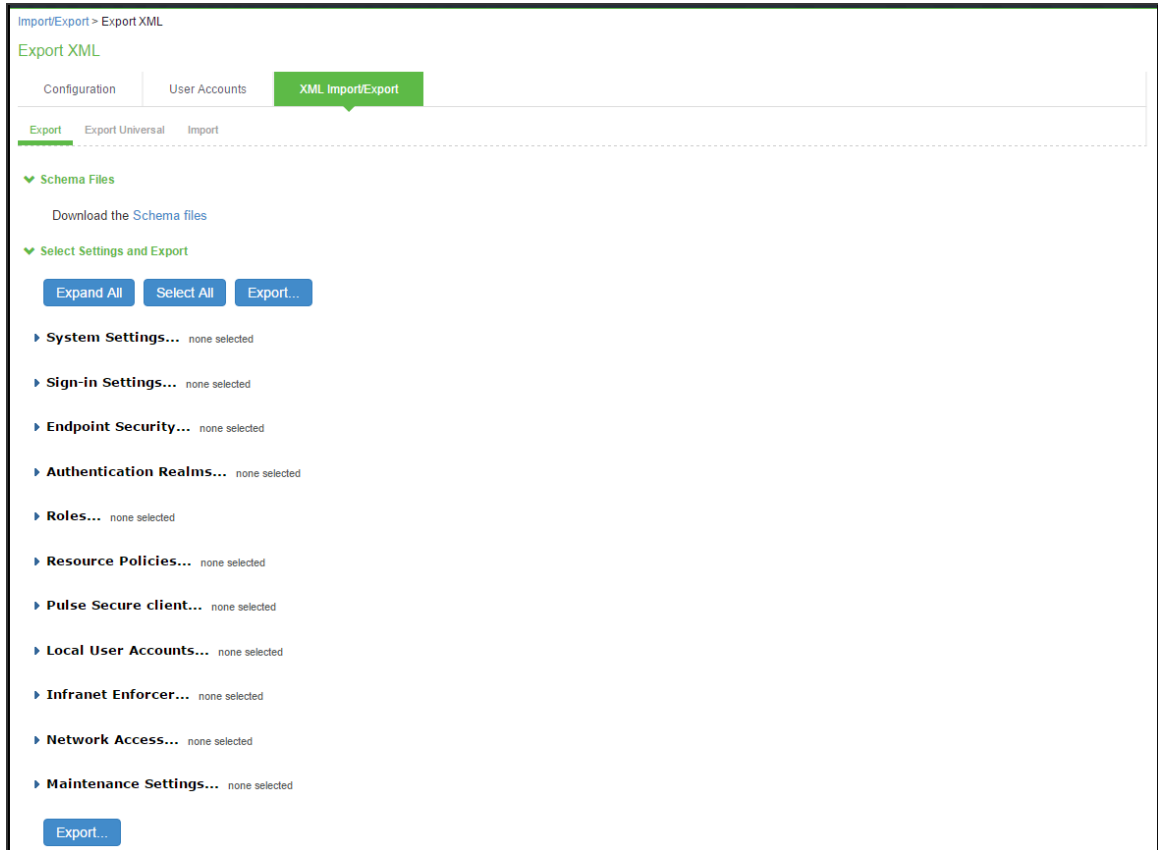
Category	Guidelines and Limitations
General	<p>The following guidelines and limitations apply:</p> <ul style="list-style-type: none"> • You can import and export configuration files only between systems running the same software version. • You might find it useful to use a text editor to modify configuration elements that ought to be distinguished, such as configuration object names and descriptions. Never modify the names of the NIC identifiers. The system relies on knowing that each appliance has two interface cards, known as NIC0 and NIC1. • Immediately after importing an Active Directory authentication server configuration, you must edit the configuration to change the Computer Object name. Unexpected problems might arise if two systems join an Active Directory domain using the same Computer Object name.
Licenses	<p>The following rules apply to exported and imported licenses:</p> <ul style="list-style-type: none"> • You cannot edit the license data that is exported. It is encrypted. • An XML import of licenses is valid only if the system does not currently have a license installed. If a license is installed already, any imported licenses are dropped. If you still intend to import a license, you must perform a factory reset before you perform the import operation.

Category	Guidelines and Limitations
	<ul style="list-style-type: none"> If you import a license after deleting a temporary license, the imported license is dropped because you might still be able to reactivate the deleted license. The import operation preserves any licensing data.
Clusters	<p>The following guidelines apply to importing a configuration file for nodes that belong to a cluster:</p> <ul style="list-style-type: none"> When you perform an import operation on a cluster, all the cluster nodes must be enabled and running. If you attempt to import a configuration into a cluster in which a node is not running, the import operation might hang or your import results might be unpredictable. The XML configuration that you import must contain the same set of nodes as the original cluster. The signature used to synchronize the cluster when the nodes are reenabled is derived from the IP addresses of the cluster nodes. Therefore, the remaining nodes cannot rejoin the cluster if the imported configuration yields a different signature. When import occurs, the imported configuration file overwrites the node-specific cluster configuration network settings of the remaining nodes. If you change the node-specific network settings, make sure you do not make the remaining nodes unreachable. After you have exported the file, do not modify settings that could render the primary node unreachable, such as changes to network settings. After you have exported the file, do not modify the XML to change the node name, IP address, or IP netmask. After you have exported the file, do not modify virtual port settings or add new virtual port settings.



To export/import an XML configuration file:

1. Select **Maintenance > Import/Export > Export/Import XML** to display the configuration page.

2. Complete the configuration and export/import operation as described in the following table.



Settings	Guidelines
Export	
Schema Files	

Settings	Guidelines
Schema files	Download the XML schema definition (.xsd) files that describe the XML.
Select Settings and Export	
Expand All	Expand the display of all settings groups.
Select All	Select all settings for all groups.
Export	Export the selected configuration data to an XML file.
Settings	
System	<p>Expand this group and select settings found under the System menu.</p> <hr/> <p> Do not select the DMI Agent unless Technical Support instructs you to do so.</p> <hr/>
Sign-in	Expand this group and select settings found under the Sign-in menu.
Endpoint Security	<p>Expand this group and select settings found under the Endpoint Security menu.</p> <hr/> <p> ESAP packages are encrypted when exported.</p> <hr/>
Authentication Realms	Expand this group and select authentication realm settings, including user realms and MAC address authentication realms.
Roles	Expand this group and select settings found under the Roles menu.
Resource Policies	Expand this group and select settings resource policies settings.
Pulse Secure	Expand this group and select settings found under the Pulse Secure menu.
Local User Accounts	Expand this group and select local authentication server settings.
Infranet Enforcer	Expand this group and select settings found under the Infranet Enforcer menu.
Network Access	Policy Secure only.
Maintenance	Expand this group and select settings found under the Maintenance menu.
Export Settings?	
Export	Export the selected configuration data to an XML file.

Settings	Guidelines
Import	
Schema Files	
Schema files	Download the XML schema definition (.xsd) files that describe the XML.
Import	
XML data file	Locate and select the XML file.
Import	Import the file. The Import XML Results page is displayed. This page contains information about the imported network settings, roles, resource policies, and other settings. If there are errors in the XML, the import operation stops and rolls back the configuration to the previous state. Error messages are displayed on the Import XML Results page.

Exporting Universal XML

The Universal Export Page is used to create XML configuration data that can be imported by either IPS or ICS. This export page only contains configuration items that can be imported by either appliance type. To export the entire configuration including appliance specific configuration data use the Export page.

Export Universal XML

Configuration | User Accounts | Profiler | **XML Import/Export**

Export | **Export Universal** | Import

The Universal Export Page is used to create XML configuration data that can be imported by either Pulse Policy Secure or Pulse Connect Secure. This export page only contains configuration from the **Export** page.

▼ **Select Settings and Export**

Expand All **Select All** **Export...**

▼ **Endpoint Security...** none selected

Select All Endpoint Settings

Host Checker
All | None

Host Checker Options
All | None

General options (interval, process-timeout, auto-upgrade, dynamic policy)

Virus Signatures list

Host Checker Policies

- None
- ALL policies
- SELECTED policies...

Remote IMV (servers and IMV)

ESAP Versions

- None
- ALL ESAPs
- SELECTED ESAPs...

▼ **Pulse Secure client...** none selected

Select All Configurations

Pulse Secure Connections

- None
- From ALL connections
- From SELECTED connections...

Pulse Secure Components

- None
- From ALL components
- From SELECTED components...

Pulse Secure Versions

- None
- From ALL versions
- From SELECTED versions...

Export

Modifying Configuration XML Files

This topic provides guidelines for modifying an exported configuration file.

Understanding the XML Export File

When you export a configuration file, the system saves the configuration as an XML file. The data in the exported file is based on the selections you make when you configure the export operation. The file contains all the required XML processing instructions and namespace declarations, which must be included exactly as defined.

Table provides some basic information and guidelines to help you understand the structured XML used in the export file.

Topic	Guideline
XML schema definition (.xsd) file	<p>The export is based on an XML schema. The schema is a separate file that defines the metadata, and that serves as a model or a template for the exported file. Use the XML schema file to:</p> <ul style="list-style-type: none"> • Identify the structure and sequence of configuration objects. • Identify optional and required elements, allowable values, default values, and other attributes of the configuration objects. <p>You can download the XML schema definition (.xsd) file in either of the following ways:</p> <ul style="list-style-type: none"> • From the XML Import/Export pages by clicking a link. • From the URL where the files are stored on the system (you do not need to sign in). <p>To access the .xsd file, access the following URL: <a href="https://<IP-or-hostname>/dana-na/xml/config.xsd">https://<IP-or-hostname>/dana-na/xml/config.xsd</p>
Elements	<p>An element is a discrete XML unit that defines an object or part of an object. The element typically consists of a pair of tags that may or may not surround string data. Tags are surrounded by angle brackets (< >).</p>
Namespaces	<p>Namespaces allow you to use the same words or labels in your code from different contexts or XML vocabularies. Prefixing elements with namespace qualifiers allows the XML file to include references to different objects that originate in different XML vocabularies and that share the same name. If you do not prefix elements with namespace qualifiers, the namespace is the default XML namespace, and you refer to element type names in that namespace without a prefix.</p> <p>When you see namespace identifiers in your XML files, you do not need to be concerned about them, as long as you do not delete or modify the identifiers.</p>

Topic	Guideline
Element Sequence	You should avoid changing the sequence of elements in the XML file, whenever possible. Although the schema does not enforce sequence in all cases, you gain no benefit from changing the order of elements from the order in which they appear in the exported file, and, in some cases, you might invalidate the XML structure by changing element sequence.

Every XML tag fits into one of the following XML tag types:

- Start tag—Defines the beginning of an element. The start tag consists of an open angle bracket (<), a name, zero or more attributes, and a close angle bracket (>). Every start tag must be followed by an end tag at some point in the document.
- End tag—Defines the end of an element. The end tag consists of an open angle bracket and a forward slash (</), followed by the same name defined in its corresponding start tag, and ends with a close angle bracket (>).
- Empty tag—The empty tag is denoted in two forms. If a tag pair has no data between them, the tag pair is considered an empty tag. Officially, according to the XML specification, an empty tag looks something like this:
<<empty tag example/>>

In this form, the empty tag consists of an open angle bracket (<), followed by an element name, a slash and a close angle bracket (>). When you see an empty tag in your configuration files, it signifies an element that the schema requires to be included in the XML file, but whose data is optional.

Start tags can contain attributes, and tag pairs (elements) can contain additional elements. The following example shows an XML file for the Users object. In this example, you see only the Administrator configuration settings.

```
<configuration xmlns="http://xml.sample.net/x">
```



```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <authentication>
    <auth-servers>
      <auth-server>
        <local>
          <users>
            <user>
              <username>admin</username>
              <fullname>Platform Administrator</fullname>
              <password-encrypted>3u+U</password-encrypted>
              <one-time-use>>false</one-time-use>
              <enabled>>true</enabled>
              <change-password-at-signin>>false</change-password-at-signin>
            </user>
          </users>
        </local>
      <name>Administrators</name>
    </auth-server>
```

You make changes to the string data that is displayed between start and end tags. For example, using the preceding example, you can add to or change the following elements:

- `<username>admin</username>`
- `<fullname>Platform Administrator</fullname>`
- `<password-cleartext>password</password-cleartext>`
- `<change-password-at-signin>>false</change-password-at-signin>`
- `<name>Administrators</name>`



The preceding sample displays the password element's data as encrypted data. You can modify the password if you change the element to password-clear text. If you modify the password, the password value is visible until it is imported back into the system. Once imported, the system encrypts the password.

If you enter passwords for new users in clear text format, the passwords are visible in the file, therefore, you might consider setting the Change Password at Next Login option to true.

- Use the password-clear text element and enter a text password when changing passwords through the XML file.



- If you change a user for a given authentication server or an authentication server for a given user, you are creating a different user, not updating an existing user or authentication server. User and authentication server together logically define a unique user.

Comparing Configuration Settings

The elements in the XML file are closely related to the objects and their options as you see them in the admin console. The element names in the XML instance file correlate closely with the displayed object and option names.

For example, select **Users > User Roles > [Role] > General > Session Options**. The admin console renders the possible values for a roaming session as an option button group, consisting of the values:

- Enabled
- Limit to subnet
- Disabled

The following snippet from the exported configuration file shows the session options for the Users role. On the bolded line, the roaming session option is disabled:

```
<session-options><SessionOptions>  
  <MaxTimeout>60</MaxTimeout>  
  <RoamingNetmask />  
  <Roaming>disabled</Roaming>  
  <PersistentSession>>false</PersistentSession>  
</SessionOptions>
```

In the schema file, you can locate the allowable values for the roaming session option:

```
<Attribute roaming:START>
<xsd:element name="roaming" minOccurs="0">
...
  <xsd:enumeration value="enabled">
...
  <xsd:enumeration value="limit-to-subnet">
...
  <xsd:enumeration value="disabled">
...
</xsd:element>
<Attribute roaming:END>
```

To change the value for the roaming session from Disabled to Limit to subnet, replace disabled with limit-to-subnet.

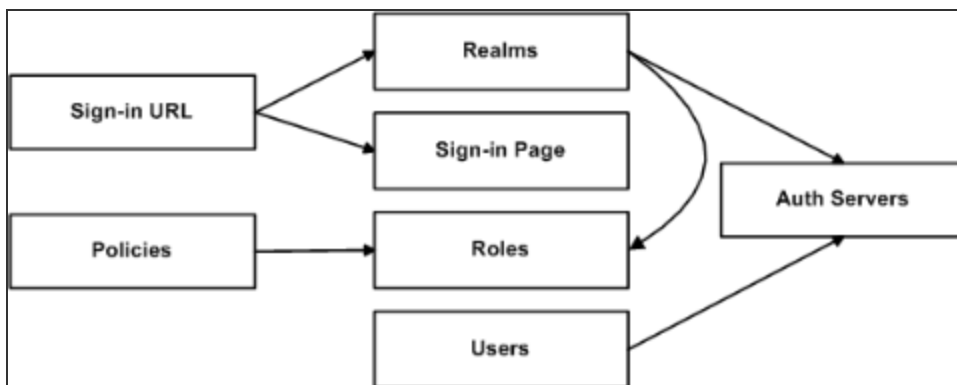
This example shows that the admin console often provides all the allowable values, displayed either in an option button group, as check boxes, as list boxes, or as other types of user interface components. The XML file displays only the current state of your configuration. The schema file displays all the actual values for the configuration options that are supported.

Understanding Referential Integrity Constraints

The system configuration objects are part of a data model that is enforced using referential integrity constraints. You cannot change these constraints, but you should understand them before you attempt to delete objects that maintain dependencies to other objects.

If you violate the referential integrity constraints, your import operation fails.

In the figure, the boxes represent object types and the arrows represent dependent relationships between the object types. Arrows point from dependent objects to objects.



The system does not allow you to delete an object on which another object depends. Conversely, when you add an object, you must add any other objects on which that object depends.

Sign-in URLs depend upon realms and sign-in pages. Realms depend upon both authentication servers and roles. Policies depend upon roles. Users depend upon authentication servers.

Consider the following scenarios based on the preceding figure:

If you add sign-in URLs, you must add realms, sign-in pages, roles, and authentication servers. You need to add an authentication server and at least one role to support the realm, and you must add the realm and the sign-in page to support the new sign-in URL.

- If you add a user, you must be able to assign it to an authentication server. If there is no authentication server on the target node yet, you must add one in the XML file.
- If you add a policy, you must be able to assign it to a role. If there is no role on the target system, you must add one in the XML file.
- If you delete an authentication server, you might strand realms and users, therefore, you need to make sure no realms or users depend on the authentication server before you attempt to delete it.
- If you delete a role, you might strand policies and realms. To delete a role, you must first delete any policy that depends upon the role, or reassign associated policies to another role. Also, to delete a role, you must first delete or reassign any realm that depends upon that role.
- If you delete a sign-in page, you might strand one or more sign-in URLs. To delete a sign-in page, you must first delete any associated sign-in URLs or reassign them to other sign-in pages.

Referential integrity checks are performed only during XML import.

Using Operation Attributes

Operation attributes define the positioning or action of XML data within the schema. If you do not specify an operation attribute, the modified data is merged by default.

XML data with an operation attribute has the following format:

```
<object1 xc:operation="operator for object1 and its children unless new operator is defined">
...
<object2>
...
<object3 xc:operation="operator for object3">
...
</object3>
...
</object2>
...
</object1>
```

The operation attribute is applied to all children objects unless a different operation attribute is defined in children objects.

The following operation attributes are supported:

- **Merge**—The configuration data identified by the element that contains this attribute is merged with the configuration at the corresponding level in the configuration datastore identified by the target parameter. This is the default behavior.
- **Replace**—The configuration data identified by the element that contains this attribute replaces any related configuration in the configuration datastore identified by the target parameter. Only the configuration present in the configuration parameter is affected.
- **Create**—The configuration data identified by the element that contains this attribute is added to the configuration if and only if the configuration data does not already exist on the device.
- **Delete**—The configuration data identified by the element that contains this attribute is deleted in the configuration datastore identified by the target parameter.
- **Insert before**—Changes the position of a configuration element in an ordered set.
- **Insert after**—Changes the position of a configuration element in an ordered set.
- **Rename**—Changes the name of one or more of a configuration object's identifiers.

If you are merging a list of objects to an existing list of objects in the configuration store, the results of the merged list might be unexpected. During a merge operation, the order of the objects in the new list is not maintained. If you are importing a list of objects and would like to preserve the order of the new list, you should use the replace operation attribute. You can also use insert before or insert after to ensure that you produce the hierarchy that you intended.

Operation attributes are applied to elements recursively unless new operators are also defined within lower-level elements. There are limitations on the legal operator that can be used in child elements without conflict with the parent operator. Table shows the legal operator relationships between parent and child elements.

Child > V-Parent	Create	Merge	Replace	Delete	Insert before	Insert after	Rename
None	OK	OK	OK	OK	OK	OK	OK
Create	OK	OK	Error	Error	OK	OK	Error
Merge	OK	OK	OK	OK	OK	OK	OK
Replace	Error	OK	OK	Error	OK	OK	Error
Delete	Error	OK	Error	OK	Error	Error	Error
Insert Before	OK	OK	OK	OK	OK	OK	OK
Insert After	OK	OK	OK	OK	OK	OK	OK
Rename	OK	OK	OK	OK	OK	OK	OK

The following examples demonstrate the import operation:

Example 1: Set the MTU to 1500 on an interface named "Ethernet0/0" in the running configuration.

```
<interface>
  <name>Ethernet0/0</name>
  <mtu>1500</mtu>
</interface>
```

Example 2: Add an interface named "Ethernet0/0" to the running configuration, replacing any previous interface with that name.

```
<interface xc:operation="replace">
  <name>Ethernet0/0</name>
  <mtu>1500</mtu>
  <address>
    <name>192.0.2.4</name>
    <prefix-length>24</prefix-length>
  </address>
</interface>
```

The default import modes have the following equivalent attributes on the root object of the configuration tree:



- Standard Import is always a merge operation.
 - Quick Import is a create operation.
 - Full Import is a replace operation.
-

Example: Importing/Exporting XML file configuration to add Multiple Users

This example shows how to use the configuration XML file import/export feature. The example is illustrative. There are additional ways to use export files.

Assume you have just added a new device to the network, and you want to add your 2,000 users to the system. Instead of adding them one at a time in the admin console, you want to perform a mass import. You can export the user accounts, extract the relevant XML that defines users, replicate each element as needed, and then import them. In this situation, your configuration should include the option to force the users to change their passwords the first time they log in to the system.

In this procedure, you only see examples for User 1, User 2, and User 2000. All other users are included in your import file. You set the passwords to numbered instances of the word password, such as password1, password2, and so on. All users in this example are assigned to the same auth server, although you can specify any combination of auth servers that are valid on your system.

To add multiple new users:

1. Select **Maintenance > Import/Export > Export XML**.
2. Follow the instructions to export local user accounts.
3. Save the exported file as users.xml.
4. Open the users.xml file.
5. Copy and paste the User container element repeatedly until you have added the necessary number of users. Although the example shows only three new users, you might add hundreds of new users to the file.
6. Update the appropriate data in each User container element as shown in [Example: Updating the User container](#).
7. Save the users.xml file.

8. Select **Maintenance > Import/Export > XML Import/Export > Import.**
9. Click **Browse** to locate and select your users.xml file.
10. Click **Import.**

Example: Updating the User container

```
<configuration xmlns="http://xml.sample.net/x/x"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<authentication>
<auth-servers>
<auth-server>
<local>
<users>
<user>
<username>user1</username>
<fullname>User1</fullname>
<password-cleartext>password1

</password-cleartext>
<one-time-use>>false</one-time-use>
<enabled>>true</enabled>
<change-password-at-signin>>true

</change-password-at-signin>
</user>
<user>
<username>user2</username>
<fullname>User2</fullname>
<password-cleartext>password2

</password-cleartext>
<one-time-use>>false</one-time-use>
<enabled>>true</enabled>
<change-password-at-signin>>true
```



```
</change-password-at-signin>
</user>
<name>System Local</name>
</auth-server>
</auth-servers>
</authentication>
</configuration>
```

Pushing the Configuration

The push configuration feature supports simple configuration management across an enterprise without requiring you to deploy the systems as a cluster. You push a partial configuration from the running configuration on the source system to the running configuration on one or more target systems.

It is not desirable to push some groups of settings to a running configuration, so the following groups of settings are not supported:

- Network configurations
- Licenses
- Cluster configurations
- Certificates
- SNMP settings
- Syslog server settings
- Push configuration targets

Guidelines and Limitations

Table summarizes the guidelines and limitations for using the push configuration feature.

Category	Guidelines and Limitations
General	The following guidelines and limitations apply:

Category	Guidelines and Limitations
	<ul style="list-style-type: none"> • You can push a configuration to systems running the same software version (same build number) or higher software version. • The source device pushes data over the management port (if configured) or the internal port. The target device can receive data over the internal or external port or management port. • You can push to a single target or to multiple targets. For example, if you install several new systems, you can push a common configuration to set their initial configuration. • When a configuration push job begins on a target, no warning is displayed, and the administrators are automatically logged out to avoid potential conflicts. • For selected configuration push, if the configuration to be pushed contains one or more JAM packages, we recommend you to push the JAM packages first considering one JAM package per push and then push the remaining configurations. • When the job has completed on a target, the target device restarts its services. Brief interrupts might occur while the service restarts. You must push to targets when they are idle or when you can accommodate brief interruptions. • You must delete the failed push jobs before performing a new push. • For entire configuration push, when pushing settings such as FIPS settings, security settings on a target even though the job has completed on a target, you might see a connection lost message on the source. You can resume the actual job to see the status and even though the source says connection lost the import will be successful.
Licenses	The push configuration job does not push licenses or licensing settings.
Clusters	<ul style="list-style-type: none"> • You can push a configuration to target that is a member of a cluster, if the target is not a member of the same cluster as the source. • You can push a configuration to multiple targets, if targets are not part of the same cluster.

Category	Guidelines and Limitations
	<ul style="list-style-type: none"><li data-bbox="483 296 1403 449">• You must not perform the clustering operations such as adding a cluster, deleting a cluster, and so on when performing a push configuration. If such events occur, then unsuccessful jobs will be aborted and the backup files will be deleted.<li data-bbox="483 489 1390 558">• You must not use VIPs during push configuration. Instead you must use the internal IP or the management IP of one of the nodes to create the target.<li data-bbox="483 598 1393 667">• You must delete the backed-up configuration on the target node(s) as soon as possible to free up the disk space.

Configuring Targets

To configure push configuration targets:

1. Select **Maintenance > Push Config > Targets** to display the target list and source options configuration page.
2. Complete the configuration for the source options as described in table.
3. Click **New Target** to display the configuration page for targets.
4. Complete the configuration as described in table.

5. Save the configuration.

Push Configuration > Targets

Targets

Push Configuration **Targets** Results History

Allow this Pulse Policy Secure to be a target
This Pulse Policy Secure will accept configuration pushed from another Pulse Policy Secure. This box must be checked on each target that is configured on this page.

Validate target server certificate
To be configured on source device. This enables source device to validate target device server certificate before pushing configuration.

[New Target...](#) [Delete...](#) [Save Changes](#)

10 records per page Search:

<input type="checkbox"/>	Target Name	Target Sign-in URL	Admin Username	Auth. Realm

Settings	Guidelines
Allow this system to be a target	Select this option to allow the system to accept configuration pushed from another system. This option must be selected on targets, but does not have to be selected on the source system.
Validate target server certificate	Select this option on the source system if you want the source system to validate the target system server certificate before pushing the configuration.
Save Changes	Click this button if you have changed the source device configuration options described above.
Delete	Select a row in the table and click Delete to remove the target from the list. You cannot delete a target if it has push configuration results associated with that target.

Push Configuration > Targets > New Target

New Target

Name: *

Sign-in URL: *

Admin Username: *

Password: *

Auth. Realm: *

[Save Changes](#)

*indicates required field

Settings	Guidelines
Name	Specify a name to identify the target within the system. Target names and target sign-in URLs cannot be edited after they have been saved.
Sign-in URL	Specify the URL for the administrator sign-in page. Sign-in URLs cannot be edited after they have been saved.
Admin Username	Specify an account on the target system that the push configuration job can use to sign-in and make changes to the configuration. The job can make wide-ranging configuration changes, so the user must have full administrative privileges. In other words, the user must belong to the Administrators role.
Password	Specify the corresponding password.
Auth. Realm	Specify the administrator authentication realm on the target system. The access management framework must be configured so that the job process (run as the username specified above) can sign in without any human interaction. For example, you cannot have dynamic credentials or multiple roles that are not merged, as these both require manual interaction. We recommend that you create an administrator account on each target that can be used exclusively for push configuration. Configure the administrator realm so that the realm policy and role mapping rules do not result in prompts requiring human interaction. For example, the user must be able to log in with static password authentication or two-factor tokens that do not use challenge-response type authentication. For example, certificates, Soft ID, and Defender Authentication are not supported.


Configuring Push Settings


To configure the settings to be pushed:

1. Select **Maintenance > Push Config > Push Configuration** to display the configuration page.

2. Complete the configuration and push configuration operation as described in the following table.

Settings	Guidelines
Select Settings and Export	
What to push	<p>Select Selected configuration or Entire configuration.</p> <p>If you select Selected configuration, the page displays controls to select settings groups.</p> <p>If you select Entire configuration, all settings from the source system are pushed, except for the following:</p> <ul style="list-style-type: none"> • Network configurations • Licenses • Cluster configurations • Certificates • SNMP settings • Syslog server settings • Push configuration targets

Settings	Guidelines
Expand All	Click this button to expand the display of all settings groups.
Select All	Click this button to select all settings for all groups.
Settings	
System	Expand this group and select settings found under the System menu. NOTE: You cannot push host-specific network settings to a target. If you want to copy these settings to another system, use the configuration XML file import/export feature.
Sign-in	Expand this group and select settings found under the Sign-in menu.
Endpoint Security	Expand this group and select settings found under the Endpoint Security menu. <hr/>  ESAP packages are encrypted when exported. <hr/>
Authentication Realms	Expand this group and select authentication realm settings, including user realms and MAC address authentication realms.
Roles	Expand this group and select settings found under the Roles menu.
Resource Policies	Expand this group and select settings resource policies settings.
Pulse Secure	Expand this group and select settings found under the Pulse Secure menu.
Local User Accounts	Expand this group and select local authentication server settings.
Infranet Enforcer	Policy Secure only. Expand this group and select settings found under the Infranet Enforcer menu.
Network Access	Policy Secure only. Expand this group and select settings found under the Network Access menu.
Maintenance	Expand this group and select settings found under the Maintenance menu.

Settings	Guidelines
Push Configuration	
Available Targets / Selected Targets	Use the Add and Remove buttons to select the targets.
Overwrite duplicate settings	Select this option to overwrite settings on the target that have the same name as settings being pushed. If you do not select this option, the push configuration job copies only configuration objects that have names different from the configuration objects on the target.
Allow Rollback to previous configuration	Select this option to revert to a previous configuration state, effectively rolling back configuration changes. If you select this option, the local configurations on the target node will be backed up before importing the configurations. You can also undo the push configuration if you want to discard the changes and revert to the previous state. We recommend you to delete the backed-up configuration if the import is successful. <hr/>  If the target configuration is large the rollback of configurations can take several minutes to complete. <hr/>
Description	Enter the description for the job. The job description is limited to 100 characters.
Schedule Import on Target	Select this option to allow a delayed import on the target node. If you select this option, the selection applies to all the targets in the job. The import schedule is measured in HH:MM (hours, minutes) format. The schedule is specified according to source's time zone.
Push Configuration	Click this button to push the selected configuration data to the specified targets. You can pause the push for a target during the push process. If errors occur during the push process, the job stops, and the configuration for the target is not imported. However, you can resume the failed push jobs. Error messages are displayed on the Results page.

Settings	Guidelines
	If you have specified multiple targets and a push configuration job to a target fails, the job continues to the next target until specified targets are updated (or fail). The results page displays the status and any problems encountered during the process.

Viewing Configuration Push Results

Purpose	The source system saves and displays the push configuration results in the Results tab.
Action	To view push configuration job results:

1. Click the Select **Maintenance > Push Config > Results** to display the results page.
2. Click a job name to display additional information about the job.
3. Select a job and click **Delete** to remove it from the results page.

The following table describes the information displayed on the Results page and the various management tasks you can perform.

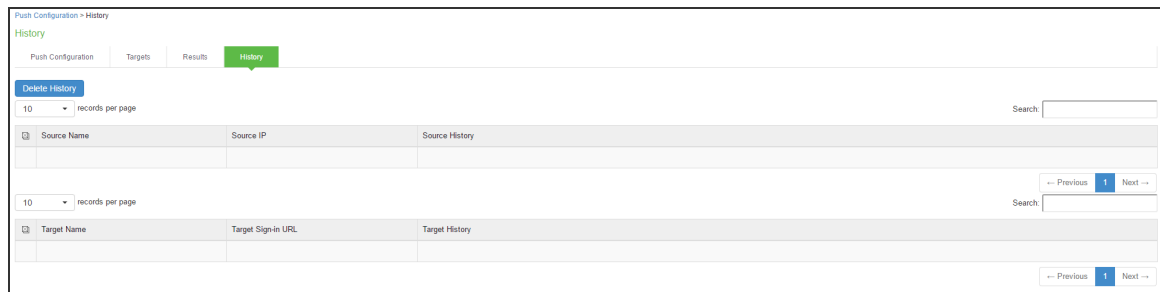
GUI Element	Guidelines
Disk Usage Details	<p>Displays the disk space available for push configuration and the disk space consumed by all the push jobs in the device.</p> <p>The disk space consumed by individual push jobs are also mentioned across each push job under the disk usage column. When total disk space consumed reaches the total disk space push jobs may fail and you can see the results column to see the failure message. You need to monitor the disk space consumed by push configuration to avoid push failures related to disk space limits.</p>
Description Column	Displays the type of the push configuration.
Disk Usage Column	Displays the disk space used by the job.
Results Column	<p>Displays the status of the transfer and result of post push action. It also displays the status of the push such as log in, export, transfer, backup, import and so on.</p> <p>The status result message shows the type of data that is getting transferred. For a paused or failed target the information on the current state of the job when it is paused, or failure reasons if any is displayed. This column also shows the progress of data transfer using a bar chart. For selected push, additional configuration data (additional configuration data refers to configuration that is transferred only if it is modified or not available on the target) includes ESAP package, JAM package, VDI configurations, Terminal services, Host Checker files, Custom sign in pages and notifications, and Applet files. For complete configuration push, additional data includes ESAP and JAM packages.</p>
Post Push Action	Displays the options that the user can perform after the push such as roll back and delete backup. It also displays the post push actions such as rollback done, backup deleted, rollback failed, performing rollback, deleting back up and so on.
Resume	Select this option to resume a paused or a failed push.
Undo	Select this option to rollback to previous configuration that was backed up. Note that you can perform this operation only when the push is successful and Allow Rollback to Previous Configuration is selected. This option is available only if the backup is not deleted or undo is not done yet.
Abort	Select this option to cancel an entire push job or push to target within a job. An aborted push cannot be resumed.

GUI Element	Guidelines
Pause	Select this option to temporarily pause the push operation to a specified target.
Delete Backup	Select this option to delete the backup configuration on the specified target. Note that this option is available only when the users selects the Allow Rollback to Previous Configuration option during the push job.

Viewing Configuration Push History

Purpose	The source/target system saves and displays up to 5 push history results per target/source in the History tab. When the history table reaches 5 entries, the system removes the oldest result data when the next push configuration job is started.
Action	To view push configuration push history:

1. Select **Maintenance > Push Config > History** to display the history page.
2. Examine the history to verify success or learn the reasons the push job failed. The history page displays rollback history however the failure reason is not displayed. You can check the failure reason in the details page for each job. It also displays the timestamp history information of successful, failed push jobs, or if a configuration is undone.
3. Select the source name and click **Delete** History to remove it from the History page.



FIPS Level 1 Support

FIPS Level 1 Support Software FIPS

Federal Information Processing Standard (FIPS) are a set of standards that define security requirements for products that implement cryptographic modules used to secure sensitive but unclassified information. The most recent standards are defined in the FIPS Publication 140-2.

The FIPS documents define, among other things, security levels for computer and networking equipment. U.S. Federal Government departments, and other organizations, use FIPS to evaluate the cryptographic capabilities of the equipment they consider for purchase. Cryptographic modules are validated against separate areas of the FIPS specification. An overall certification level is assigned based on the minimum level achieved in any area. Although primarily aimed at environments requiring strict security, FIPS levels are increasingly enforced as qualifying criteria for all U.S. Federal Government contracts. Security-conscious private enterprises might also use FIPS levels as an equipment evaluation benchmark. FIPS levels also serve as a customer-neutral description of vendor requirements. Vendors can engineer security products to FIPS levels and extend the applicability and eligibility of these products across a broad customer base, thereby eliminating exhaustive and time-consuming customer-by-customer product qualification procedures.

Ivanti offers FIPS level 1 support for IPS. Both services use a 140-2 level 1 certified cryptographic module to comply with FIPS. When FIPS level 1 support is enabled applications, such as browsers, accessing the web server must support Transport Layer Security (TLS), the latest version of Secure Socket Layer (SSL). If the platform features hardware acceleration, then for SSL processing SSL hardware acceleration is disabled as hardware acceleration does not comply with FIPS validation. Only FIPS approved algorithms are used when in FIPS level 1 support is enabled.

For more information about the Ivanti Cryptographic Module, see the [security policy](#) and the [validation certificate](#). For a complete list of validated FIPS 140-1 and FIPS 140-2 cryptography modules, see <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#2018>.

FIPS Supported Platforms

The following platforms support FIPS level 1:

- PSA 300/3000/5000/7000
- IPS virtual appliances

FIPS Level 1 Support

Once you enable FIPS level 1 support, your browser is restricted to specific custom cipher strengths. A list of supported ciphers is shown during the enabling process.

When you enable FIPS level 1 support, the following events occur on the system:

- The Web server restarts and turns on FIPS level 1 support. The Web server now allows only TLSv1.0, TLSv1.1 and TLSv1.2 protocols that include FIPS approved cryptographic algorithms which include Suite B cipher suites.



Once FIPS level 1 support is enabled, new client sessions will use FIPS if the client supports FIPS. Existing client sessions may not be using FIPS. To ensure FIPS capable clients are in FIPS level 1 support, all client sessions should be terminated after the FIPS level 1 support is enabled. Administrators can use the **System > Status > Active Users** page to terminate client sessions.

- If the platform features hardware acceleration, when FIPS level 1 support is enabled SSL processing does not utilize the hardware acceleration. IPsec hardware acceleration is not affected.

The following event logs are generated for FIPS level 1 support:

- SYS30966 when the web server turns FIPS level 1 support on.
- ADM30965 when the administrator turns FIPS level 1 support on or off.
- ERR30967 when the web server fails to turn on FIPS level 1 support.

To enable FIPS level 1 support:

1. Select **System > Configuration > Inbound SSL Options**.
2. Under SSL FIPS Mode option, select **Turn on FIPS mode**.

Configuration > Security > SSL Options

SSL Options

Configuration
Security

Licensing Pulse One **Security** Certificates DMI Agent Guest Access Notification

Inbound SSL Options Outbound SSL Options Health Check Options Miscellaneous Advanced

DoD Certification option
When this option is enabled, the web service will be placed in JITC Mode. NDcPP and FIPS Modes will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart.

Turn on JITC mode

SSL NDcPP Mode option
When this option is enabled, the web service will be placed in NDcPP Mode. FIPS Mode will also be turned on and all non-FIPS ciphers will be disabled. The web service will restart. NDcPP Mode is a prerequisite for JITC Mode.

Turn on NDcPP mode

SSL FIPS Mode option
When this option is enabled, the web service will be placed in FIPS Mode, the cipher strength will be set to Medium, and all non-FIPS ciphers will be disabled. The current cipher customization might be lost. The web and RADIUS services will restart. FIPS mode is a prerequisite for NDcPP Mode.

Turn on FIPS mode

Inbound Settings

Allowed SSL and TLS Version
The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS. It is no longer supported.

Accept only TLS 1.2 and later (maximize security)
 Accept only TLS 1.1 and later
 Accept only TLS 1.0 and later
 Accept SSL V3 and TLS (maximize compatibility)

Allowed Encryption Strength
Strong ciphers (rated by the number of bits in the cipher) improve the security of SSL encryption, but some browsers may only support 40-bit ciphers. When there is more than one acceptable cipher, the Pulse Policy Secure will give preference to the cipher with the fastest data transfer rate, regardless of its relative encryption strength. Changing the encryption strength will cause the web service to restart. Please see the Setting Security Options section in the Admin guide for more details.

PFS - Perfect Forward Secrecy
 SuiteB - Accept only SuiteB ciphers (Requires an ECC certificate)
 Maximize Security (High Ciphers)
 Maximize Compatibility (Medium Ciphers)
 Custom SSL Cipher Selection

▶ Show Selected Ciphers

Encryption Strength option
Normally, the allowed encryption strength is enforced after an SSL session is established, so that a user that connects using a disallowed encryption strength will receive a web page describing the problem. The option below will prevent a browser with a weak cipher from establishing a connection. Changing this option will cause the web service to restart.

Do not allow connections from browsers that only accept weaker ciphers

Key Exchange Options
If the Allowed Encryption Strength includes any DH ciphers, the system uses 1024bit DHE key exchange by default. The option below will increase key exchange strength to 2048bit DHE.

Use 2048bit Diffie-Hellman key exchange

SSL Legacy Renegotiation Support option
When this option is enabled, renegotiation with clients and servers, which dont support the new TLS Renegotiation Info extension (defined in RFC 5746), will be allowed. When disabled, renegotiation with such clients and servers will not be allowed. Changing this option will cause the web service to restart.

Enable support for SSL legacy renegotiation

Common options

SSL Handshake Timeout option
By default, the SSL handshake has a timeout of 60 seconds. Use the text box below to set a different value.

Timeout: seconds 10-600 seconds

Note that changing any of the above settings might restart some services in the Pulse Policy Secure.

[Save Changes](#)

Once you turn on FIPS level 1 support, the following changes are made:

- Under Allowed SSL and TLS Version, the **Accept only TLS** option is selected.
- Under Allowed Encryption Strength, **Maximize Compatibility (Medium Ciphers)** is set. Only FIPS approved ciphers are selected. See Supported Cipher Suites when FIPS Level 1 Support is Enabled and Disabled
- Under Encryption Strength, the **Do not allow connections from browsers that only accept weaker ciphers** option is selected.

3. Click **Save Changes**.

FIPS Level 1 support is now enabled on the device. If your browser does not support any of the listed ciphers, you will not be able to log in to the device.

When enabling FIPS mode on IPS, only the following protocols are FIPS compliant:

- EAP-TTLS
- EAP-PEAP
- EAP-TLS

A warning is displayed if non-FIPS protocols are configured on an IPS FIPS enabled device. However, these protocols are not disabled as they may be required for other use cases such as for the MAC authentication bridge.

Entries are made in the Events logs to show that FIPS level 1 support is enabled.

The screenshot displays the 'Log/Monitoring > Events > Logs' interface. The 'Events' tab is selected, showing a list of logs with columns for Log, Settings, and Filters. The 'View by filter' is set to 'Standard:Standard (default)' and 'Show' is set to '200' items. The 'Edit Query' field is empty, with 'Update', 'Reset Query', and 'Save Query...' buttons below it. Below the query field are buttons for 'Save Log As...', 'Clear Log', 'Save All Logs', and 'Clear All Logs'. The 'Filter:Standard (default)' and 'Date:Oldest to Newest' are shown. The 'Export Format:Standard' is also visible. The log entries are as follows:

Level	Message ID	Timestamp	Source	Message
Info	SYS30966	2012-11-11 21:32:20	ive - [127.0.0.1] System()	- FIPS Mode Set for web server
Minor	SYS10306	2012-11-11 21:32:19	ive - [127.0.0.1] System()	- Starting services: web server
Info	ADM30965	2012-11-11 21:32:13	ive - [127.0.0.1] System()	- FIPS Mode is now turned on. The web server will restart.

FIPS Level 1 Support

Problem: If you have FIPS level 1 support enabled and your browser does not support the required cipher suites, you cannot access the device. If this happens to an administrator account, you can no longer administer or configure the system.

Solution: You can turn off FIPS level 1 support and reset the encryption strength from the device's serial console. After choosing that option, SSL options are reset to Accept only TLS 1.0 and later and to **Maximize Compatibility (Medium Ciphers)**.

Open a serial console to your device and select option 8. **Turn off FIPS Mode and reset allowed encryption strength for SSL.**

Turning Off FIPS Level 1 and Resetting Encryption Strength from the Serial Console

Please choose the operation to perform:

1. Network Settings and Tools
2. Create admin username and password
3. Display log/status
4. System Operations
5. Toggle password protection for the console (Off)
6. Create a Super Admin session.
7. System Maintenance
8. Turn off FIPS Mode and reset allowed encryption strength for SSL
Choice: 8



Once you turn off FIPS level 1 support, option 8 is relabeled "Reset allowed encryption strength for SSL."

Supported Cipher Suites

When FIPS level 1 support is enabled, only TLSv1.0, v1.1, v1.2 and AES256, 3DES and AES128 are allowed. The order of the cipher suites is not dependent on the SSL hardware acceleration module since hardware acceleration is not used when FIPS level 1 support is enabled.

When FIPS level 1 support is enabled, the following settings are automatically configured:

- In the SSL Options window:
 - Under Allowed SSL and TLS Version, the **Accept only TLS** option is selected. All other options under this section are disabled.
 - Under Allowed Encryption Strength, the **Maximize Compatibility (Medium Ciphers)** option is selected. Only FIPS approved ciphers are selected.
 - Under Encryption Strength Option, the **Do not allow connections from browsers that only accept weaker ciphers** option is selected.
- SSL hardware acceleration is disabled. IPsec hardware acceleration is not affected by the FIPS level 1 support being enabled.

The first four cipher suites in the below table are given preference due to the requirements in RFC 6460. The first two cipher suites meeting the requirement for Suite B Profile for TLS 1.2. The next two meeting the requirement for Suite B Transitional Profile for TLS 1.0 and 1.1.

Cipher Suite	Protocol
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	TLSv1.0 and later
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and later
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and later

Cipher Suite	Protocol
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.0 and later
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.0 and later

Cipher Suite	Protocol
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1.0 and later
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and later
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1.0 and later
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2

Cipher Suite	Protocol
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS1.0 and later
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS1.0 and later

Cipher Suite	Protocol
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1.0 and later
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and later
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1.0 and later
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS1.0 and later
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS1.0 and later

Cipher Suite	Protocol
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and later
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and later
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	TLS1.0 and later

Dashboard and Reports

Dashboard and Report Overview

A dashboard is an interface used to manage the Pulse Secure access management framework. It provides an integrated view of all devices and users accessing the network, their device profile information, authentication methods used to gain access, device posture compliance and so on.

A report is an element of a dashboard used to convey complex data in simplified formats. Pulse Secure access management framework collects log and configuration data from across your network, and it then aggregates the data into reports for you to view and analyze. It provides a standard set of predefined reports that you can use and customize to fit your needs. The reports are grouped into logical categories for information related to authentication, session traffic, device administration, configuration and administration, and troubleshooting.

You can use the system dashboard and reports to analyze system utilization.

Enabling the Dashboard

You can use the admin console to enable or disable the dashboard.

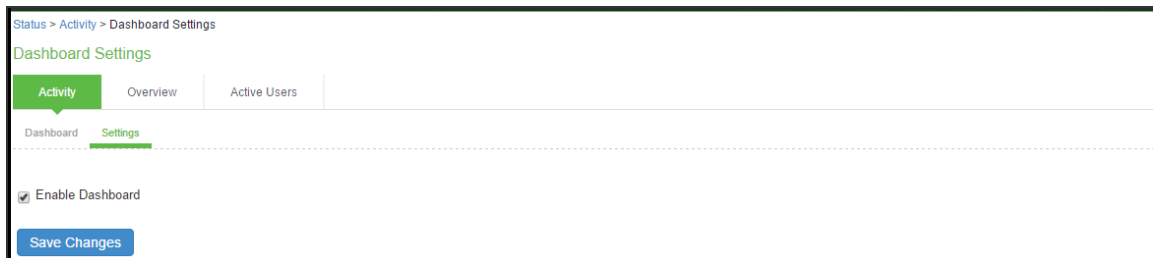
To enable the dashboard.

1. Select **System > Status > Activity > Settings**.
2. Select **Enable Dashboard**.



The dashboard is enabled by default.

The following figure shows the dashboard settings for IPS.



Using the Dashboard

Dashboard Overview

The dashboard contains six default graphic reports focused on security, network activity, application activity, system monitoring, and compliance.

Metric	Description
Policy Secure	
Total Endpoints	The total number of unique endpoints over a time. If an endpoint provides a unique identifier (mobile device ID, client ID, and so on), then it will be used to identify the endpoint. For a browser-based session where an identifier is not available, each session is considered a unique endpoint.
Active Endpoints	The total number of unique endpoints with active sessions.
Active Guests	The total number of active guest users. A guest user is defined as a user with an expiration date. This includes administrator-created and GUAM-created guest users. This does not include GUAM-created users without expiration dates.
Active MAC Auth Users	The total number of active MAC authentication users.

Table describes the default dashboard charts.

Dashboard Chart	Description
Authentication Success	The number of successful authentications over the selected time (1, 7, or 30 days). The 7-day chart is a bar graph. The 1-day and 30-day charts are line graphs.
Authentication Failure	The number of failed authentications over the selected time (1, 7, or 30 days). The 7-day chart is a bar graph. The 1-day and 30-day charts are line graphs.
Session OS Count	Pie chart showing the number of the sessions per operating system.

Dashboard Chart	Description
Top Roles	Pie chart showing the number of top user roles assigned during the selected time.
Compliance Results	Pie chart showing Host Checker posture assessment results: Compliant, Not Compliant, Not Assessed, or Remediated. Compliance results are reported for all instances in which Host Checker is run. The posture assessment chart is clubbed with the compliance results chart for IPS. To view the posture assessment chart, select Posture Assessment from the dropdown list.
Posture Assessment	Pie chart showing Host Checker policy violations. Policy violations are reported only for instances in which Host Checker is run at initial sign in.
Auth Mechanism	Pie chart showing the number of sessions per authentication mechanism: 802.1x, Layer 3, MAC address. It applies to IPS only.

Dashboard Database

The dashboard monitoring service collects and stores data in a database for 30 days. The total number of records stored in the database can be up to 300,000 records.

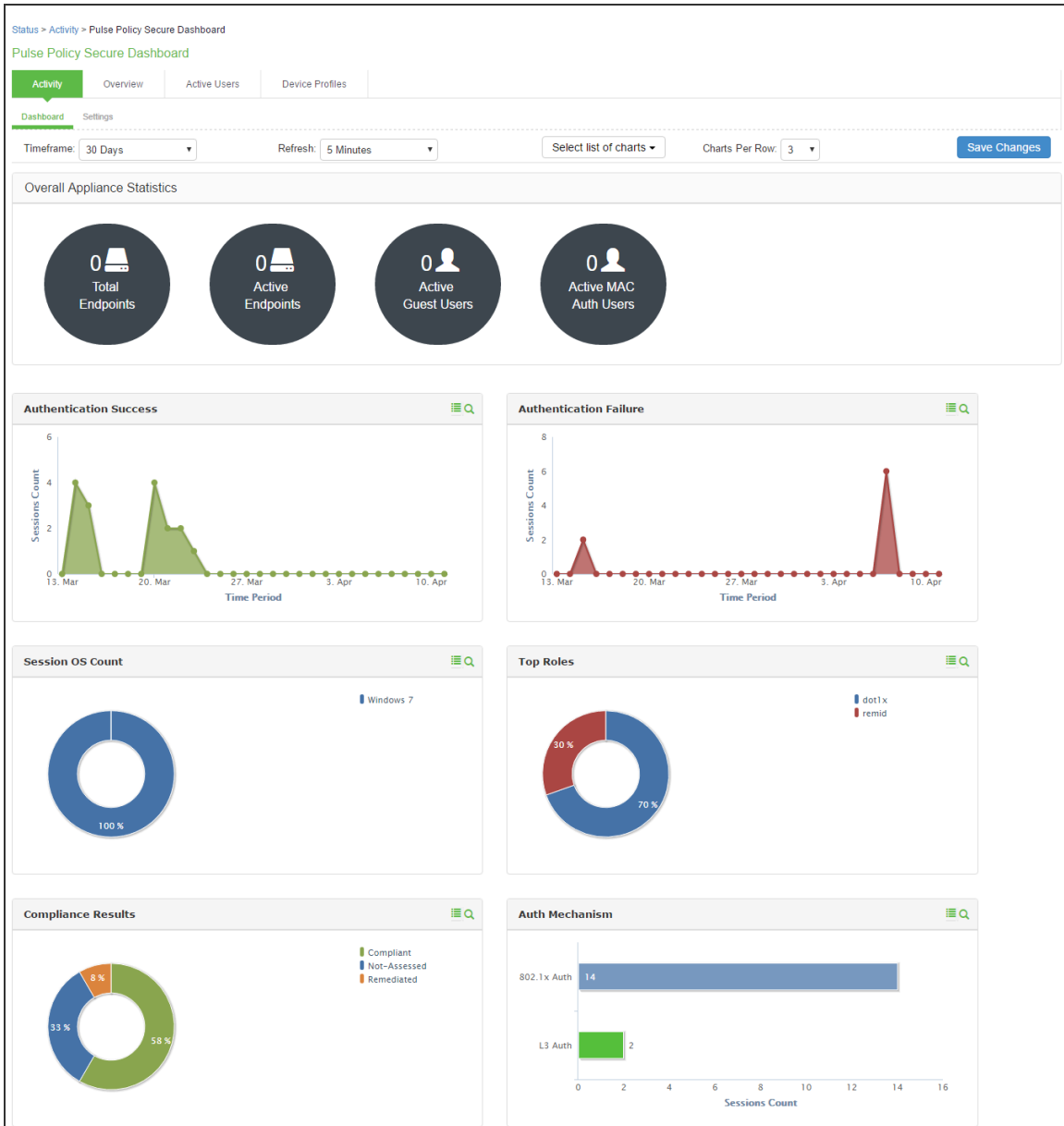
The dashboard database is created only after upgrading to IPS version 5.0 or later and enabling the dashboard option. Note that only new sessions are added to the database and changing the Time Frame filter or clicking refresh sends queries to the database. The data is collected only when the dashboard option is enabled.

Table describes the different actions and their results.

Action	Description
Disable and then reenble the dashboard.	The data collection stops when your dashboard is disabled.
Restore the data from backup, snapshot, or import config.	The data is not exported and the data is retained during upgrades

Displaying the Dashboard

To display the dashboard, select **System > Status > Activity > Dashboard**.



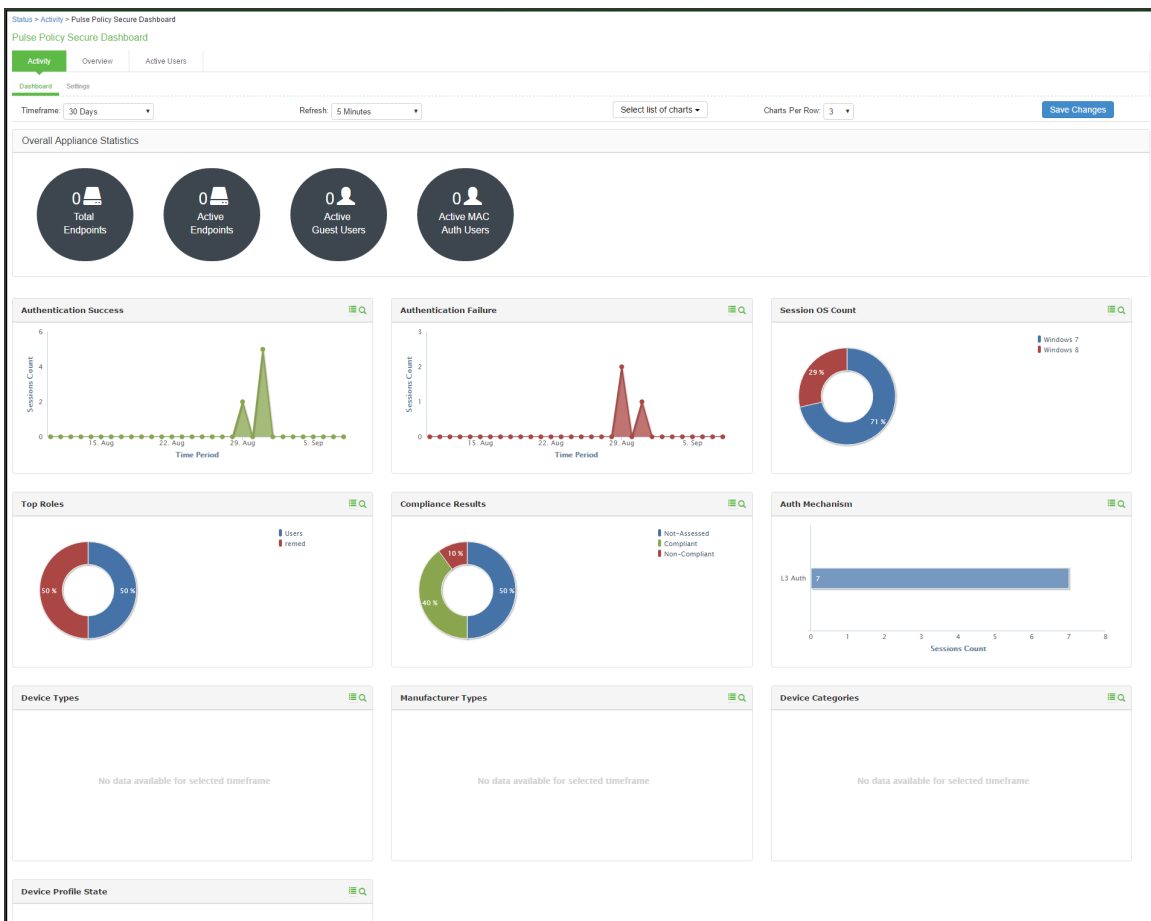
Selecting a Data Time Frame

To select a data timeframe:

1. Select **System > Status > Activity > Dashboard**.
2. Select one of the following periods from the Time Frame list box:
 - **Last 24 Hours**– (Default) Refers to the last 24 hours from the current hour.
 - **Last 7 Days**– Refers to current day and the previous last 6 days.
 - **Last 30 Days**– Refers to current day and the previous last 29 days.



Access records are kept for 30 days. Older records are removed and not included in dashboard charts and reports.



Refreshing Data

To refresh data:

1. Select **System > Status > Activity > Dashboard**.
2. Select one of the following refresh rates from the Refresh list box:
 - Disabled
 - 5 Minutes
 - 10 Minutes
 - 30 Minutes
 - 60 Minutes

Drilling Down to Detailed Reports

To drill down to view detailed reports:

1. Select **System > Status > Activity > Dashboard**.
2. Click the search icon to display the corresponding tabular report with predefined search filters. For example, enter the filter criteria with the Authentication Results set to Success.

Schedule Report or Email Scheduling

IPS allows you to schedule email notification for sending customized reports. Admin can configure email frequency and select one of the saved filters for getting a customized report.

To schedule reports:

1. Select **System > Configuration > Notification > Email Scheduler** or **Schedule report** option in the reports page.
2. Enter the name for the email schedule rule.
3. Under Email Settings, enter the email address either from **General Settings** or **Custom** option.
4. Click **Test Settings** to test the email settings.

5. Configure the email schedule frequency for running the email schedule.
 - **Daily** – Generates reports daily at 7 AM.
 - **Weekly** – Generates reports every Monday at 7 AM.
 - **Monthly** – Generates reports on 1st of every month at 7 AM.
 - **Custom** – Generates reports based on date and time selected.
6. Under **Report Settings**, select the report type from the drop-down.
7. If Device Discovery Report is selected, the following 2 options appear.
 - **Generate Full Report**- If selected, full (stats) report is generated rather than incremental report. If unselected, Incremental reports are generated based on the email schedule. For example, if Weekly is selected, the reports will be generated based on the last one week activity on the Profiler.
 - **Generate Device Discovery Report**- If selected a filter drop-box appears. Device Discovery Report is generated along with the Profiler statistics in PDF format. If unselected, only Profiler statistics will be sent.
8. Choose the desired filter. See [Creating a new Filter](#) section for information on how to create filters. The corresponding saved filters gets populated automatically.
9. Click **Save Changes**.

The newly created email rule gets listed in the email rules table. The reports will be generated based on the selection and emailed. The existing email schedule can also be edited or deleted based on your requirement.



The scheduled email reports will be sent based on IPS server time.
Only one email schedule can be configured for one report at a time.

Configuration > Notification > Email Scheduler

Email Scheduler

Licensing Pulse One Security Certificates DMI Agent Sensors Client Types SAML Guest Access Advanced Networking **Notification**

General **Email Scheduler**

* Name:

Email Settings

Set appropriate schedule and emails to receive Detailed reports (PDF format), in your inbox.

Use emails from General Settings Custom

The emails will be sent to following email addresses:

[Test Settings](#)

SMTP server configuration is required for sending emails. Currently SMTP Server is configured and enabled. [Click here](#) to change the settings.

* Email Schedule: **Weekly** Select an option based on your email schedule frequency.
Every Monday - 7AM.

Reports Settings

* Report: **Device Discovery**

Generate Full Report Select an option based on your email schedule frequency. Select the checkbox if full reports needs to be generated every time.

Generate Device Discovery Report Select the checkbox if Device Discovery reports needs to be generated every time.

Select Filters: **DDR-manufacture**

[Save Changes](#) [Reset](#)

* indicates required field

[Delete](#)

<input type="checkbox"/>	Name	Email ID	Report	Filter	Schedule
<input type="checkbox"/>	SUA	shobhalid@publ...	Single User Activities	SUA_7Days	Daily
<input type="checkbox"/>	DS	...	Device Summary	DS_7Days	Daily

Authentication Report

Pulse Secure Reports

Prepared for:
Pulse Policy Secure

Version:
9.1R11-5499

Report on Pulse Profiler:
0320M2AWK0NDS111E ()

Appliance type:
PSA-5000

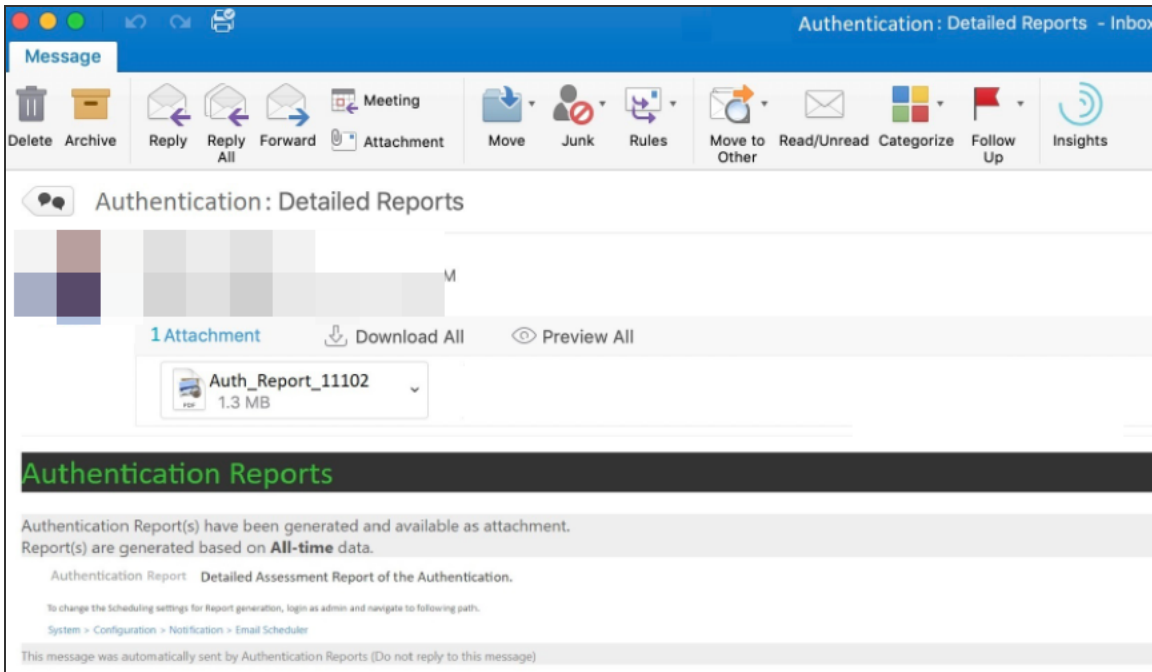
Report Date:
Wed Feb 03 01:30:36 GMT 2021

Report Timeframe:
Jan 04, 2021 - Feb 03, 2021





S.No.	Username	Realm	Login Time	Auth Mechanism	Auth Result	Failure Reason	Device Id	Role	Device OS	IP Address	MAC Address
1	pulse		Fri, 29 Jan 13: 22:42 2021	L3 Auth	Failure	No Realm	e852a7c449a4449b767d9c344974a72		Mac OS	10.96.74.89	08-6D-41-B5-C3-46



Using the User Summary Report

This topic describes the user summary report. It includes the following information:

Overview

The user summary report displays user statistics such as realm, username, last log in time, last log in IP, successful log in, and so on for each user based on the user activity in the selected time range.

To display the user summary report, select **System > Reports > User Summary**.

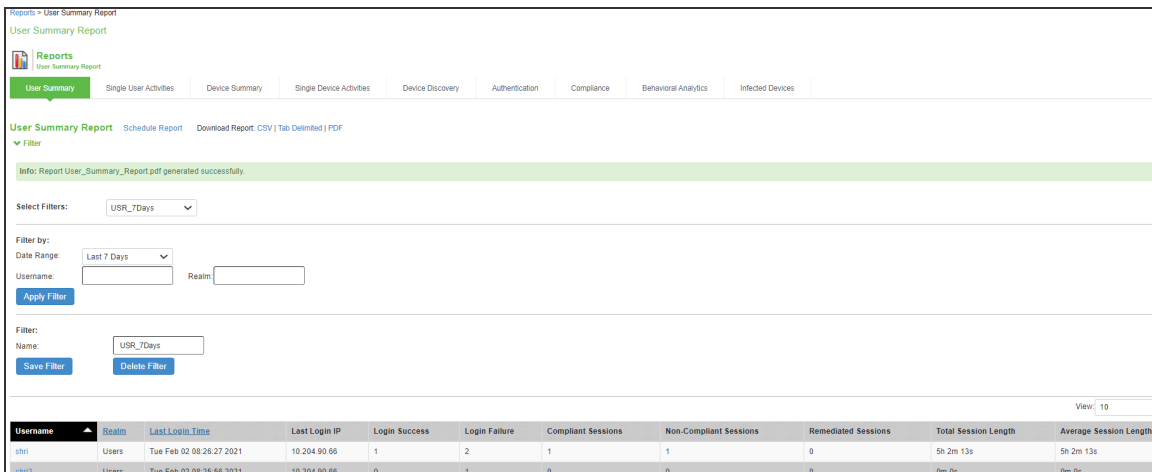


Table describes the columns on the user summary report.

Column	Description
Username	Specifies the name of the user.
Realm	Specifies the realm.
Last Login Time	Specifies the last time the user logged in.
Last Login IP	Specifies the last IP that the user logged in with.
Login Success	Specifies the number of successful log ins.
Login Failure	Specifies the number of failed log ins.
Compliant Sessions	Specifies the number of compliant sessions.
Non Compliant Sessions	Specifies the number of non compliant sessions.
Remediated Sessions	Specifies the number of remediated sessions.
Total Session Length	Specifies the total length of the sessions.
Average Session Length	Specifies the average length of the sessions.

Creating a new Filter

To create a new filter:

1. Select **System > Reports > User Summary**.
2. Under Filter, enter the name of the filter.

3. Under Filter by: Select one of the following periods from the Date Range list box:
 - **Last 24 Hours**– (Default) Refers to the last 24 hours from the current hour.
 - **Last 7 Days**– Refers to current day and the previous last 6 days.
 - **Last 30 Days**– Refers to current day and the previous last 29 days.
 - **Custom**– Enter the custom from and till date range.
4. Enter search criteria in one or more of the following attribute columns:
 - Username
 - Realm
5. Click **Save Filter**.

Once the filter is created, it gets listed in the filter drop-down. Administrator can also choose to edit the existing filter to customize the report based on the requirement. The filter can also be deleted using the Delete Filter option.

Applying Data Filters

To apply a data filter:

1. Select **System > Reports > User Summary**.
2. Select one of the following periods from the Date Range list box:
 - **Last 24 Hours**– (Default) Refers to the last 24 hours from the current hour.
 - **Last 7 Days**– Refers to current day and the previous last 6 days.
 - **Last 30 Days**– Refers to current day and the previous last 29 days.
 - **Custom**– Enter the custom from and till date range.
3. Enter search criteria in one or more of the following attribute columns:
 - Username
 - Realm
4. Click **Apply Filter**.

Sorting Records

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data columns or multiple columns.

To sort the user summary report

1. Select **System > Reports > User Summary**.
2. Select one of the following columns from the user summary report table and click either the ascending or descending order icon.
 - Username
 - Realm
 - Last Login Time



The username column is sorted in ascending order by default.

Drilling Down to the Single User Report

To drill down to a single user report:

1. Select **System > Reports > Single User Activities**.
2. Enter the username and specify the data range.
3. Click **Apply Filter**.

Exporting User Summary Report

To export device summary report:

1. Select **System > Reports > User Summary**.
2. Select a Download Report option.
 - **CSV**– Exports the report in CSV format.
 - **Tab Delimited**– Exports the report in tab-delimited format.
 - **PDF**– Exports the report in PDF format.

Using the Device Summary Report

This topic describes the device summary report.

Overview

The device summary report displays device information such as device detail, MAC address, last log in time, last log in IP, log in successful, and so on for each user based on device activity in the selected time range.

To display the device summary report select **System > Reports > Device Summary**.

Device ID	MAC Address	Last Login Time	Last Login IP	Last Login Username	Login Success	Login Failure	Compliant Sessions	Non-Compliant Sessions	Remediated Sessions	Total Session Length	Average Session Length
00:50:56:43:F:E:09		Tue Feb 02 08:26:27 2021	10.204.99.66	stn1	1	3	1	1	0	5h 2m 13s	5h 2m 13s

The following table describes the columns on the device summary report.

Column	Description
Device ID	Specifies a unique identifier to identify the endpoint. Click the device ID icon to view a single device report.

Column	Description
MAC Address	Specifies the MAC address of the device. Click the MAC address to view a single device report.
Last Login Time	Specifies the last time the device was logged in.
Last Login IP	Specifies the last IP that the device logged in with.
Last Login Username	Specifies the username that the user logged in with.
Login Success	Specifies the number of successfully log ins.
Login Failure	Specifies the number of failed log ins.
Compliant Sessions	Specifies the number of compliant sessions.
Non-Compliant Sessions	Specifies the number of non-compliant sessions.
Remediated Sessions	Specifies the number of remediated sessions.
Total Session Length	Specifies the total session length.
Average Session Length	Specifies the average session length.



If a device has more than one MAC address in a session, then the value appearing in the MAC Address column will be multiple instead of the actual MAC addresses. Note that the value multiple is not hyperlinked.

Creating a new Filter

To create a new filter:

1. Select **System > Reports > User Summary**.
2. Under Filter, enter the name of the filter.
3. Under Filter by: Select one of the following periods from the Date Range list box:
 - **Last 24 Hours**– (Default) Refers to the last 24 hours from the current hour.
 - **Last 7 Days**– Refers to current day and the previous last 6 days.
 - **Last 30 Days**– Refers to current day and the previous last 29 days.
 - **Custom**– Enter the custom from and till date range.
4. Enter search criteria in one or more of the following attribute columns:
 - Last Login Username
 - Mac Address
5. Click **Save Filter**.

Once the filter is created, it gets listed in the filter drop-down. Administrator can also choose to edit the existing filter to customize the report based on the requirement. The filter can also be deleted using the Delete Filter option.

Applying Data Filters

To apply a data filter:

1. Select **System > Reports > Device Summary**.
2. Select one of the following periods from the Date Range list box:
 - **Last 24 Hours**– (Default) Refers to the last 24 hours from the current hour.
 - **Last 7 Days**– Refers to current day and the previous last 6 days.
 - **Last 30 Days**– Refers to current day and the previous last 29 days.
 - **Custom**– Enter the custom from and till date range.

3. Enter search criteria in one or more of the following columns:
 - Last Login Username
 - Mac Address
4. Click **Apply Filter**.

Sorting Records

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data columns or multiple columns.

To sort the device summary report

1. Select **System > Reports > Device Summary**.
2. Select any one of the following column and click either the ascending or descending order icon.
 - Last Login Time
 - Last Login Username

You can sort the column in either ascending order or descending order.

Exporting Device Summary Report

To export device summary report:

1. Select **System > Reports > Device Summary**.
2. Select a Download Report option.
 - **CSV**– Exports the report in CSV format.
 - **Tab Delimited**– Exports the report in tab-delimited format.
 - **PDF**– Exports the report in PDF format.

Using the Single Device Report

This topic describes the single device report.

Overview

The single device activities report displays the device activity information such as username, realm, log in time, log out time, device detail, MAC address, authentication mechanism, authentication result, compliance, IP address, role and so on for each device.

To display the single device activities report, select **System > Reports > Single Device Activities**.

Username	Realm	Login Time	Logout Time	Duration	Device ID	MAC Address	Auth Mechanism	Auth Result	Compliance	IP Address	Role	Device Detail
shri	Users	Tue Feb 02 08:26:27 2021	Tue Feb 02 13:28:40 2021	5h 2m 13s		00-50-56-83-FE-09	L3 Auth	Success	Compliant	10.204.90.66	Users	
shri	Users	Tue Feb 02 08:26:24 2021				00-50-56-83-FE-09	L3 Auth	Failure Failure Reason: Short Password	Not-Assessed	10.204.90.66		

Table describes the columns on the single device report.

Column	Description
Username	Specifies the name of the user.
Realm	Specifies the realm.
Login Time	Specifies the time the user logged in.
Logout Time	Specifies the time the user logged out.
Duration	Specifies the total duration of the user session.
Device ID	Specifies a unique identifier used to identify an end point. Click the device ID icon to view a single device report.
MAC Address	Specifies the MAC address of the device.
Auth Mechanism	Specifies the authentication mechanism: 802.1x, Layer 3, MAC address.

Column	Description
Auth Result	Specifies the authentication result.
Compliance	Specifies the Host Checker posture assessment results: Compliant, Not Compliant, Not Assessed, or Remediated.
IP Address	Specifies the IP that the user logged in with.
Role	Specifies the role of the user.
Device Detail	Displays the URL that is used for connecting to the MDM server.

Creating a new Filter

To create a new filter:

1. Select **System > Reports > User Summary**.
2. Under Filter, enter the name of the filter.
3. Under Filter by: Select one of the following periods from the Date Range list box:
 - **Last 24 Hours**– (Default) Refers to the last 24 hours from the current hour.
 - **Last 7 Days**– Refers to current day and the previous last 6 days.
 - **Last 30 Days**– Refers to current day and the previous last 29 days.
 - **Custom**– Enter the custom from and till date range.
4. Enter search criteria in one or more of the following attribute columns:
 - Compliance Results
 - MAC Address
 - Device ID
 - Authentication Mechanism (L3 Auth, 802.1X Auth, MAC auth, all)
5. Click **Save Filter**.

Once the filter is created, it gets listed in the filter drop-down. Administrator can also choose to edit the existing filter to customize the report based on the requirement. The filter can also be deleted using the Delete Filter option.

Applying Data Filters

To apply a data filter:

1. Select **System > Reports > Single Device Activities**.
2. Select one of the following periods from the Filter by: Date Range list box:
 - **Last 24 Hours**– (Default) Refers to the last 24 hours from the current hour.
 - **Last 7 Days**– Refers to current day and the previous last 6 days.
 - **Last 30 Days**– Refers to current day and the previous last 29 days.
 - **Custom**– Enter the custom from and till date range.
3. Enter search criteria in one or more of the following columns:
 - Compliance Results
 - MAC Address
 - Device ID
 - Authentication Mechanism (L3 Auth, 802.1X Auth, MAC auth, all)
4. Click **Apply Filter**.

Sorting Records

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data column.

To sort the single device activities report:

1. Select **System > Reports > Single Device Activities**.
2. Select Login Time column and click either the ascending or descending order icon.
3. You can sort the column in either ascending order or descending order.

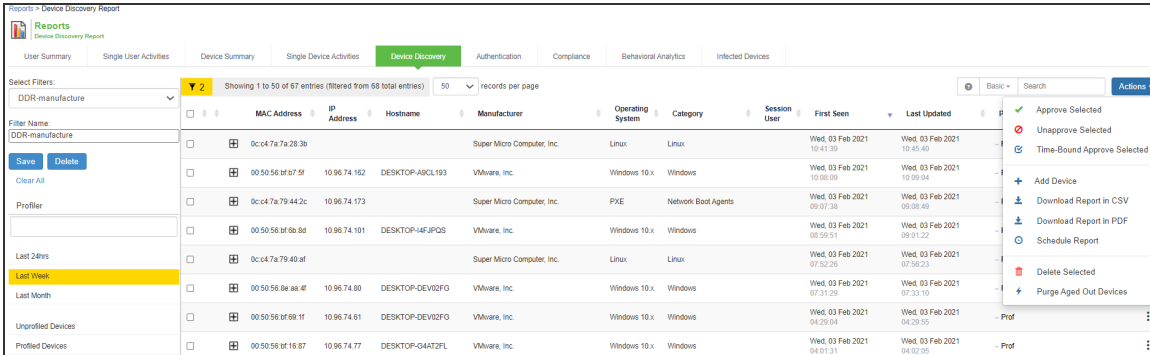
Exporting Single Device Activities Report

To export single device activities report:

1. Select **System > Reports > Single Device Activities**.
2. Select a Download Report option.
 - **CSV**– Exports the report in CSV format.
 - **Tab Delimited**– Exports the report in tab-delimited format.
 - **PDF**– Exports the report in PDF format.

Using the Device Discovery Report

You can view the device discovery report if you have integrated Profiler with IPS. The Device Discovery Report contains the list of devices that are discovered in the network. Select **System > Reports > Device Discovery** to view the report.



MAC Address	IP Address	Hostname	Manufacturer	Operating System	Category	Session User	First Seen	Last Updated	Actions
0c:c4:7a:7a:28:3b			Super Micro Computer, Inc.	Linux	Linux		Wed, 03 Feb 2021 10:41:39	Wed, 03 Feb 2021 19:45:40	Approve Selected Unapprove Selected Time-Bound Approve Selected
00:50:56:bf:b7:5f	10.96.74.162	DESKTOP-ABCL193	VMware, Inc.	Windows 10.x	Windows		Wed, 03 Feb 2021 10:08:09	Wed, 03 Feb 2021 10:09:04	+ Add Device
0c:c4:7a:79:44:2c	10.96.74.173		Super Micro Computer, Inc.	PXE	Network Boot Agents		Wed, 03 Feb 2021 09:07:38	Wed, 03 Feb 2021 09:08:49	Download Report in CSV Download Report in PDF Schedule Report
00:50:56:bf:6b:8d	10.96.74.101	DESKTOP-I4FJPO8	VMware, Inc.	Windows 10.x	Windows		Wed, 03 Feb 2021 09:08:51	Wed, 03 Feb 2021 09:09:25	
0c:c4:7a:79:40:af			Super Micro Computer, Inc.	Linux	Linux		Wed, 03 Feb 2021 07:52:26	Wed, 03 Feb 2021 07:56:23	Delete Selected
00:50:56:bf:aa:4f	10.96.74.80	DESKTOP-DEV02FG	VMware, Inc.	Windows 10.x	Windows		Wed, 03 Feb 2021 07:31:29	Wed, 03 Feb 2021 07:33:10	Purge Aged Out Devices
00:50:56:bf:09:1f	10.96.74.61	DESKTOP-DEV02FG	VMware, Inc.	Windows 10.x	Windows		Wed, 03 Feb 2021 04:29:04	Wed, 03 Feb 2021 04:29:55	- Prof
00:50:56:bf:16:87	10.96.74.77	DESKTOP-GAATZFL	VMware, Inc.	Windows 10.x	Windows		Wed, 03 Feb 2021 04:01:31	Wed, 03 Feb 2021 04:02:09	- Prof

To view more information about a profiled device, click the + icon to the left of the MAC address. See *Profiler Deployment Guide* for more information.

Using the Authentication Report

This topic describes the authentication report.

Overview

The authentication report displays the authentication result for each user based on the device activity in the selected time range.

Displaying the Authentication Report

To display the authentication report, select **System > Reports > Authentication**.

Username	Realm	Login Time	Auth Mechanism	Auth Result	Failure Reason	Device ID	Role	Device OS	IP Address	MAC Address
shri	Users	Tue Feb 02 08:26:27 2021	L3 Auth	Success			Users	Windows 10	10.204.90.66	00-50-56-83-FE-09
shri	Users	Tue Feb 02 08:26:24 2021	L3 Auth	Failure	Short Password			Windows 10	10.204.90.66	00-50-56-83-FE-09

Table describes the columns on the authentication report.

Column	Description
Username	Specifies the name of the user.
Realm	Specifies the realm.
Login Time	Specifies the time the user logged in.
Auth Mechanism	Specifies the authentication mechanism: 802.1x, Layer 3, MAC address.
Auth Result	Specifies the authentication result.
Failure Reason	Specifies the host checker failure reason.
Device ID	Specifies a unique identifier used to identify an end point. Click the device ID icon to view a single device report.
Role	Specifies the user role.
Device OS	Specifies the operating system of the device.
IP Address	Specifies the IP Address of the device.
MAC Address	Specifies the MAC Address of the device.

Creating a new Filter

To create a new filter:

1. Select **System > Reports > User Summary**.
2. Under Filter, enter the name of the filter.
3. Under Filter by: Select one of the following periods from the Date Range list box:
 - **Last 24 Hours**– (Default) Refers to the last 24 hours from the current hour.
 - **Last 7 Days**– Refers to current day and the previous last 6 days.
 - **Last 30 Days**– Refers to current day and the previous last 29 days.
 - **Custom**– Enter the custom from and till date range.
4. Enter search criteria in one or more of the following attribute columns:
 - Authentication Mechanism
 - Authentication Results
 - Username
 - Realm
 - IP Address
 - Mac Address
 - Roles
5. Click **Save Filter**.

Once the filter is created, it gets listed in the filter drop-down. Administrator can also choose to edit the existing filter to customize the report based on the requirement. The filter can also be deleted using the Delete Filter option.

Applying Data Filters

To apply a data filter:

1. Select **System > Reports > Authentication**.
2. Select one of the following periods from the Filter by: Date Range list box:
 - **Last 24 Hours**– (Default) Refers to the last 24 hours from the current hour.
 - **Last 7 Days**– Refers to current day and the previous last 6 days.
 - **Last 30 Days**– Refers to current day and the previous last 29 days.
 - **Custom**– Enter the custom from and till date range.
3. Enter search criteria in one or more of the following columns:
 - Authentication Mechanism
 - Authentication Results
 - Username
 - Realm
 - IP Address
 - Mac Address
 - Roles
4. Click **Apply Filter**.

Sorting Records

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data column.

To sort the authentication report:

1. Select **System > Reports > Authentication**.
2. Select **Login Time column** and click either the ascending or descending order icon.

Exporting Authentication Report

To export an authentication report:

1. Select **System > Reports > Authentication**.
2. Select a Download Report option.
 - **CSV**– Exports the report in CSV format.
 - **Tab Delimited**– Exports the report in tab-delimited format.
 - **PDF**– Exports the report in PDF format.

Using the Compliance Report

This topic describes the compliance report.

Overview

The compliance report displays compliance status such as compliant, not compliant, remediated, not assessed information for each user based on the device activity in the selected time range.

To display the compliance report, select **System > Reports > Compliance**.

The screenshot shows the 'Compliance Report' page in a web application. At the top, there are navigation tabs: 'User Summary', 'Single User Activities', 'Device Summary', 'Single Device Activities', 'Device Discovery', 'Authentication', 'Compliance' (highlighted), 'Behavioral Analytics', and 'Infected Devices'. Below the tabs, there are options to 'Schedule Report' and 'Download Report' in CSV, Tab Delimited, or PDF formats. A 'Filter' section is visible with a dropdown menu set to 'Compliance_7Days'. Below this, there are fields for 'Filter by: Date Range' (set to 'Last 7 Days') and 'Compliance Results' (with a dropdown menu showing 'Compliant', 'Non-Compliant', 'Remediated', and 'Not-Assessed'). There are also input fields for 'Username' and 'MAC Address', and a 'Realms' dropdown. At the bottom, there are buttons for 'Apply Filter', 'Save Filter', and 'Delete Filter'. A table at the bottom displays the report data with columns: Username, Realm, Device ID, MAC Address, Session Compliance, Initial Host Check Time, and Initial Host Check Details.

Username	Realm	Device ID	MAC Address	Session Compliance	Initial Host Check Time	Initial Host Check Details
shri	Users		00-50-56-83-FE-09	Compliant	Tue Feb 02 08:28:27 2021	Host check result: Pass

Table describes the different columns on the compliance report.

Column	Description
Username	Specifies the name of the user.
Realm	Specifies the realm.
Device ID	Specifies a unique identifier used to identify an end point. Click the device ID icon to view a single device report.
MAC Address	Specifies the MAC address of the device.
Session Compliance	Specifies the Host Checker posture assessment results: Compliant, Not Compliant, Not Assessed, or Remediated.
Initial Host Check Time	Specifies the initial host check time.
Initial Host Check Details	Specifies the host check result.

The posture assessment chart is also a part of compliance report. It is displayed based on Initial Host Checker evaluation details (Login time).

Table lists the type and the failure reasons for Host Checker.

Type	Failure Reason
Antivirus	Anti-virus not installed Anti-virus not running Anti-virus not up to date Anti-virus scan time check failed
Firewall	Firewall not installed Firewall not running
Antimalware	Anti-malware not installed
Antispyware	Anti-spyware not installed Anti-spyware not running
OS Checks	Unsupported OS
Port	Restricted ports open Required ports not open

Type	Failure Reason
Process	Detected restricted processes Required processes not detected
File	Detected restricted files Required files missing
Registry	Incorrect registry settings
NetBIOS	Detected restricted NetBIOS names Required NetBIOS names not found
MAC Address	Detected restricted MAC address Required MAC address not present
Machine Certificate	Certificate missing
Patch Assessment	Patches missing
Cache Cleaner	Cache cleaner failed
Remote IMV	Remote IMV failure
3rd party	NA (Not considered for reporting)
3rd party sub policy	3rd party sub policy failed
Rooting Detection	Detected rooted devices
Jail Breaking Detection	Detected jail broken devices
3rd party NHC Check	Generic failure

Type	Failure Reason
Statement of Health	Generic failure
Connection Control	Generic failure

Type	Failure Reason
HC	HDEncryption software not installed Detected Unencrypted drives Drives are missing Unsupported client for HDEncryption check Patch Management software not installed Detected missing patches Unsupported client for PatchMgmt check Deprecated patch assessment rule

Creating a new Filter

To create a new filter:

1. Select **System > Reports > User Summary**.
2. Under Filter, enter the name of the filter.
3. Under Filter by: Select one of the following periods from the Date Range list box:
 - **Last 24 Hours**– (Default) Refers to the last 24 hours from the current hour.
 - **Last 7 Days**– Refers to current day and the previous last 6 days.
 - **Last 30 Days**– Refers to current day and the previous last 29 days.
 - **Custom**– Enter the custom from and till date range.
4. Enter search criteria in one or more of the following attribute columns:
 - Compliance Results
 - Username
 - Realm
 - MAC Address
5. Click **Save Filter**.

Once the filter is created, it gets listed in the filter drop-down. Administrator can also choose to edit the existing filter to customize the report based on the requirement. The filter can also be deleted using the Delete Filter option.

Applying Data Filters

To apply a data filter:

1. Select **System > Reports > Compliance**.
2. Select one of the following periods from the Filter by: Date Range list box:
 - **Last 24 Hours**– (Default) Refers to the last 24 hours from the current hour.
 - **Last 7 Days**– Refers to current day and the previous last 6 days.
 - **Last 30 Days**– Refers to current day and the previous last 29 days.
 - **Custom**– Enter the custom from and till date range.
3. Enter search criteria in one or more of the following columns:
 - Compliance Results
 - Username
 - Realm
 - MAC Address
4. Click **Apply Filter**.

Sorting Records

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data column.

To sort the compliance report:

1. Select **System > Reports > Compliance**.
2. Select **Initial Host Check Time** or Username column and click either the ascending or descending order icon.

Exporting Compliance Report

To export a compliance report:

1. Select **System > Reports > Compliance**.
2. Select a Download Report option.
 - **CSV**– Exports the report in CSV format.
 - **Tab Delimited**– Exports the report in tab-delimited format.
 - **PDF**– Exports the report in PDF format.

Using the Infected Devices Report

This topic describes the infected devices report.

Overview

The infected devices report displays infected device details such as MAC address, user name, IP address, device status information.

To display the compliance report, select **System > Reports > Infected Devices**.

Reports > Infected Devices

Infected Devices

Reports
Infected Devices Report

User Summary | Single User Activities | Device Summary | Single Device Activities | Device Discovery | Authentication | Compliance | Behavioral Analytics | **Infected Devices**

Infected Devices Report | Schedule Report | Download Report: CSV | Tab Delimited | PDF

▼ Filter

Select Filters:

Filter by:

Device Status: |

Username:

IP Address: | MAC Address:

Filter:

Name:

*Below listed devices are permanently blocked or quarantined as per Admission Control policy

MAC Address	Username	IP Address	Blocked By	Device Status
-------------	----------	------------	------------	---------------

Table describes the different columns on the infected devices report.

Column	Description
Username	Specifies the name of the user.
MAC Address	Specifies the MAC address of the infected device.
IP Address	Specifies the IP address of the infected device.
Blocked By	Specifies the component, which blocked the infected device. For example, client.
Device Status	Specifies the device status of the infected device.

Creating a new Filter

To create a new filter:

1. Select **System > Reports > Infected Devices**.
2. Under Filter, enter the name of the filter.
3. Under Filter by: Select the device status from the list box:
 - **Blocked**
 - **Quarantined**
4. Enter search criteria in one or more of the following attribute columns:
 - Username
 - IP Address
 - MAC Address
5. Click **Save Filter**.

Once the filter is created, it gets listed in the filter drop-down. Administrator can also choose to edit the existing filter to customize the report based on the requirement. The filter can also be deleted using the Delete Filter option.

Exporting Infected Devices Report

To export a infected device report:

1. Select **System > Reports > Infected Devices**.
2. Select a Download Report option.
 - **CSV**– Exports the report in CSV format.
 - **Tab Delimited**– Exports the report in tab-delimited format.
 - **PDF**– Exports the report in PDF format.

System Maintenance

Overview

The system maintenance operations must be planned to ensure that your system functions properly and to avoid any network disruptions. You can check the IPS platform information and perform the required tasks, which includes upgrading or downgrading the software, downloading the client installer files, performing disk cleanup operations and so on.

The system maintenance menu includes the following components:

- Platform- Use this option to check the platform information such as model, version, serial number, current version, and the rollback version. This helps the Administrator to perform/plan any routine system maintenance operations.
- Upgrade/Downgrade- Use this option to upgrade/downgrade the IPS software.
- Change Personality- Use this option to change the personality of the IPS device to a ICS device.
- Options- Use this option to check the global system parameters, including hardware settings.
- Installers- Use this option to download the client installer files based on the user platform.

Configuring System Platform

The platform page provides a quick overview of the current state of the system. This gives a quick overview of what Operation System the system has booted, the fallback version, host name, hardware model, serial number, uptime, current version, and the rollback version.

The screenshot shows the 'Platform' page in the System Maintenance interface. It includes a navigation menu with 'Platform', 'Upgrade/Downgrade', 'Change Personality', 'Options', and 'Installers'. The main content area displays system details such as Hostname (localhost2), Model (MAG-4610), Serial Number (0274082011000012), Uptime (94 days, 1 hour, 46 minutes, 6 seconds), Current version (5.4R1), and Rollback version (5.3R5:HF1). Below this, there are buttons for 'Restart Services', 'Reboot...', 'Shut Down...', and 'Rollback...'. A 'Connectivity' section includes a 'Test Connectivity' button. A 'Hardware Status' section shows a table for 'Fan Status' with two fans, both showing a green status indicator. At the bottom, the temperature is listed as 21 °C.

To restart, reboot, rollback or shut down the system:

1. Select **Maintenance > System > Platform** to display the system maintenance platform page.
2. Click the desired node operation:
 - **Restart**—Kills all processes and restarts the system. The system is available again after a few minutes.
 - **Reboot**—Power cycles and reboots the system. The system is available again after a few minutes.
 - **Shut Down**—Shuts down the system. The system is not available again until the physical power button on the physical device is used to restart the system.
 - **Rollback**- The system is rolled back to the previous software version and configuration state. The system is rebooted and unavailable for a few minutes when you rollback.

- The restart, reboot, and shutdown operations are applied to all enabled members of a cluster. If you do not want to apply the operations to all members of the cluster, use the System > Clustering > Status page to disable members; then perform the restart, reboot, or shut down operation.



- If you have enabled logging for Administrator changes (System > Log/Monitoring > Admin Access > Settings page), a log is written to the Admin Access logs page. If you have enabled logging for System Status (System > Log/Monitoring > Events > Settings page), logs are written to the Events logs page.

Configuring System Maintenance Options

You can use the maintenance options page to enable various system maintenance features.

To enable various system maintenance features:

1. Select **Maintenance > System > Options** to display the maintenance options page.
2. Select options as described in table.
3. Save the configuration.

System Maintenance > Options

Options

Platform Upgrade/Downgrade Change Personality **Options** Installers

Automatic version monitoring
By enabling this feature, you allow the retention of any data regarding usage and performance statistics to be used by Pulse Secure, including for improvement of future versions of the product and related support. The data is transmitted over a secure (SSL) connection.

Enable gzip compression
Use gzip compression to reduce the amount of data sent to browsers that support HTTP compression. This can result in faster page downloads for some users.

Enable Kernel Watchdog
Enables the kernel watchdog that automatically restarts the system under kernel deadlock or when kernel runs low on some key resources.

Enable File System Auto-clean Feature
Enables the system to automatically clean up the file system when disk utilization reaches 90%. IMPORTANT: when enabled, this feature may result in loss of data that may be relevant in debugging system problems that occurred a week or earlier in the past (i.e. old debuglogs, core files, and snapshots may be removed.)

Enable web installation and automatic upgrade of Odyssey Access Clients



Enable web installation and automatic upgrade of Pulse Secure clients
By default, the Policy Secure automatically installs and upgrades UAC agents (Odyssey or Pulse clients) of users who have connected to it. These options can be used to enable/disable the automatic installation and upgrade of the UAC agent. Uncheck this option only if you intend to manage installation and upgrade of the UAC agent through some other mechanism (for more information, refer to the documentation).

End-user Localization: Automatic (based on browser settings) ▾

▶ External User Records Management

Save Changes

Options	Guidelines
Automatic version monitoring	<p>If you enable this option, the system reports the following data to IPS:</p> <ul style="list-style-type: none"> • Machine identifier.

Options	Guidelines
	<ul style="list-style-type: none"> • Information describing your current software, including: <ul style="list-style-type: none"> • Software build number and build name. • An MD5 hash of your license settings. • An MD5 hash of the internal interface IP address. • If this node is in a cluster, the number of nodes within that cluster. • Current state of the node. • Cluster type (active/active, active/passive). • Total number of unique subnets on the cluster nodes. • Version of Ivanti Policy Secure. • Version of ESAP. • Cluster log synchronization status. • Number of Infranet Enforcers configured • Names of RADIUS vendors configured • Total number of concurrent users on the device. <p>We strongly recommend that you enable this service.</p>
Kernel Watchdog	<p>Enables the kernel watchdog that automatically restarts the system under kernel deadlock or when kernel runs low on some key resources.</p> <hr/> <p> Enable the kernel watchdog only when instructed by Ivanti Global Support Center.</p> <hr/>
File System Auto-clean	<p>Enables the system to automatically clean up the file system when disk utilization reaches 90%.</p> <hr/> <p> The clean-up operation deletes files that might be relevant in debugging—for example, debug logs, core files, and snapshots might be deleted.</p> <hr/>

Options	Guidelines
Web installation and automatic upgrade of Pulse Clients	<p>After you deploy Pulse Client software to endpoints, software updates occur automatically. A Pulse client can receive updates from the server. If you upgrade the Pulse software on your Pulse server, updated software components are pushed to a client the next time it connects.</p> <p>A bound endpoint receives connection set options and connections from its binding server, but it can have its Pulse client software upgraded from any Pulse server that has the automatic upgrade option enabled. During a client software upgrade the client loses connectivity temporarily.</p>
Virtual Terminal console	Enables the virtual terminal on a virtual appliance. Clear this check box to use the serial console. Changing this setting will restart the system.
End-user Localization	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Automatic (based on browser settings) • English (U.S.) • Chinese (Simplified) • Chinese (Traditional) • French • German • Japanese • Korean • Spanish
External User Records Management	
Persistent user records limit	<p>Specify the maximum number of user records.</p> <p>This feature is useful when system performance is affected due to many user records. We highly recommend you consult Ivanti Global Support Center prior to using this feature. Deleting a user record removes all persistent cookies, SSO information, and other resources for that user. It does not remove the user record from the external or internal authentication server. If you delete a user record and that user logs back in to the authentication server, new user records are created. Records are not removed if that user is currently logged in.</p>

Options	Guidelines
Number of records to delete when the limit is exceeded	Specify a number. Older records are removed first. A user record is not deleted if that user is currently logged in.
Delete records now	Check whether the persistent user records limit has been exceeded. If it is, delete the number of user records specified in the option above.
Automatic deletion of user records during new user log ins	Check whether the persistent user records limit will be exceeded whenever a new user record is about to be created. If true, delete the records prior to creating the user new record.

Installing the Service Package

This topic describes how to upgrade, downgrade, and rollback the system software.

Downloading and Uploading the Software Package

To download a software package:

1. Go to <http://www.pulsesecure.net/support/downloads> and browse to the software download page for your product.
2. When prompted, log in with your Ivanti customer username and password.
3. Accept the license agreement.
4. When prompted, save the software package to your local host.

You can upload a software package to the system without immediately initiating the upgrade process. This is known as staging the upgrade. You can stage one package. Uploading a second package overwrites the previous staging.

To upload a software package:

1. Select **Maintenance > System > Upgrade/Downgrade** to display the system software maintenance page.
2. Under Managed Staged Service Package, select Upload new package into staging area and use the Browse button to locate and select the service package file.
3. Click **Submit** to upload the file.

The Upload Status window shows the progress of the upload operation.



If you have enabled logging for Administrator changes (**System > Log/Monitoring > Admin Access > Settings** page), a log is written to the Admin Access logs page.

Upgrading the System Software

Installing a service package can take several minutes and requires the system to reboot. Because existing system data is backed up during this process, you can decrease installation time by clearing your system log before trying to install a service package.



- When the system software is upgraded the latest set of updated Trusted Server CAs are uploaded. These new set of Trusted Server CAs can be seen in the **System > Configuration > Certificates > Trusted Server CAs** page. The expired certificates are removed from the system.
- When the system software is upgraded, it automatically upgrades IPS to OpenSSL version 1.0.2n.

To upgrade the operating system:

1. Select **Maintenance > System > Upgrade/Downgrade** to display the system software maintenance page.
2. Under Install Service Package, select one of the following options to proceed:
 - **From File**—Use the Browse button to locate and select the service package file.
 - **From Staged Package**—Select the service package file that was previously uploaded.



Do not select the **Deletes** option when you are upgrading software. The Deletes option is available to support downgrading software.

3. Click **Install**.

The system displays the Service Package Installation Status page, which provides a summary of the integrity checks and compatibility checks and other status indicators.

Service Package Installation Status

The installation process takes a few minutes. When complete, the system needs to reboot. Please wait...

- Step 1: Verifying package integrity complete (32 seconds)
- Step 2: Extracting install script complete (43 seconds)
- Step 3: Extracting install script complete (14 seconds)
- Step 4: Preparing disk partitions complete (1 seconds)
- Step 5: Extracting contents of new package complete (14 seconds)
- Step 6: Saving package complete (14 seconds)
- Step 7: Finalizing installation complete (23 seconds)
- Step 8: Encrypting drive please wait complete (96 seconds)
- Step 9: Switching current system to "rollback" and enabling new system ... complete (1 seconds)

Installation completed successfully and the system will now reboot. Note that the Administrator Console will be unavailable while the system reboots.(Watch the serial console for messages).
When the system reboots click [here](#) to continue using the Administrator Console.



If you have enabled logging for Administrator changes (**System > Log/Monitoring > Admin Access > Settings page**), a log is written to the **Admin Access** logs page. If you have enabled logging for System Status (System > Log/Monitoring > Events > Settings page), logs are written to the Events logs page.

Downgrading the System Software

If necessary, you can downgrade to an earlier version of the system software. When you downgrade, you must clear the system and configuration data to avoid unexpected behavior that can occur when the system has data that relates to the newer software.

If you downgrade the system, you must reestablish network connectivity before you can reconfigure it.

To downgrade the operating system:

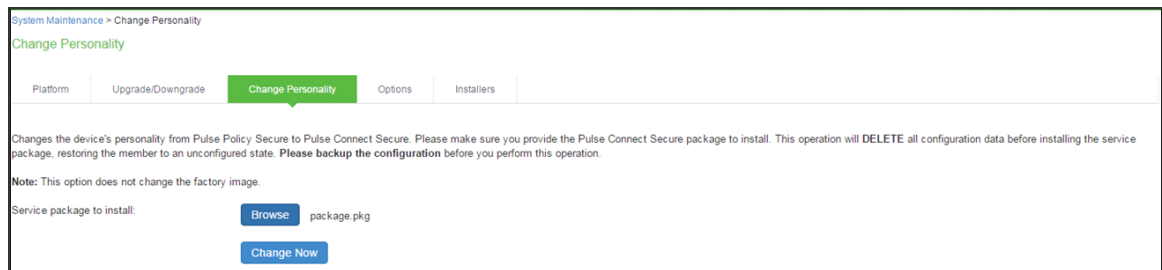
1. Select **Maintenance > System > Upgrade/Downgrade** to display the system software maintenance page.
2. Under Install Service Package, select one of the following options to proceed:
 - **From File**—Use the Browse button to locate and select the service package file.
 - **From Staged Package**—Select a service package file that was previously uploaded.
3. Select the Deletes all system and user configuration data option to delete all system and user configuration data before installing the service package, restoring the member to an unconfigured state.
4. Click **Install**.

Changing the Device Personality

You can use this page to change the device's personality from IPS to ICS. You must perform a backup operation to avoid losing the configuration data before using this configuration.

To change the device personality:

1. Click **Browse** and select the **ICS service package to install**.
2. Click **Change Now**.



Downloading Client Installer Files

You can use the system maintenance client installers page to download client installer files. The downloadable files include .exe and .msi files for use installing clients on Windows platforms, and .dmg files for installing clients on Macintosh platforms.

To download client installer files:

1. Select **Maintenance > System > Installers** to display the client installer files page.
2. Click **Download** to download the file to your local host.

The screenshot shows the 'System Maintenance > Installers' page. The 'Installers' tab is selected. The page lists several installer files with their descriptions and version information.

File Name	Description	Version	Action
Pulse Secure Installer Service (.exe)	This component simplifies future installation and upgrades of Pulse Secure's client software for users with limited desktop privileges. Use this self-extracting .exe package unless a specific requirement exists for Microsoft Windows Installer (msi) packages. This package can be deployed with limited user privileges if a previous version of the Installer Service is running.	version: 9.0R3.1 (build 51667)[9.0.3-51667(3011)]	[Download]
Pulse Secure Installer Service (.msi)	This component simplifies future installation and upgrades of Pulse Secure's client software for users with limited desktop privileges. Deploy this Microsoft Windows Installer (msi) package if your organization or infrastructure requires msi packages. One such example would be automated software installation using Microsoft Systems Management Server.	version: 9.0R3.1 (build 51667)[9.0.3-51667(3011)]	[Download]
Host Checker	This component verifies security settings on user's workstation.	version: 9.0R3.1 (build 51667)[9.0.3-51667(3011)]	[Download]
Third-party Integrity Measurement Verifier (IMV) Server	This component allows third-party integrity measurement verifiers (IMV's) to be used with the Pulse Policy Secure	version: 9.0R3.1 (build 51667)[9.0.3-51667(3011)]	[Download]
Agent (32-bit)	This component authenticates user, conducts host check, and provides optional encrypted transport to Enforcer. Please consult the Pulse Secure Supported Platforms Guide for this version to determine which versions of Windows 32-bit client operating systems are supported.	version: 4.4.20.41795	[Download]
Agent (64-bit)	This component authenticates user, conducts host check, and provides optional encrypted transport to Enforcer. Please consult the Pulse Secure Supported Platforms Guide for this version to determine which versions of Windows 64-bit client operating systems are supported.	version: 4.4.20.41795	[Download]
Pulse Secure Installer (Windows 32-bit)	This setup application installs all Pulse Secure components. Please consult the Pulse Secure Supported Platforms Guide for this version to determine which versions of Windows 32-bit client operating systems are supported.	version: 9.0.3.1599	[Download]
Pulse Secure Installer (Windows 64-bit)	This setup application installs all Pulse Secure components. Please consult the Pulse Secure Supported Platforms Guide for this version to determine which versions of Windows 64-bit client operating systems are supported.	version: 9.0.3.1599	[Download]
Pulse Secure Installer (MacOS)	This setup application installs all Pulse Secure components. Please consult the Pulse Secure Supported Platforms Guide for this version to determine which versions of MacOS client operating systems are supported.	version: 9.0.3.1599	[Download]
Pulse Application Launcher Installer	This setup application installs all Pulse Application Launcher components.	version: 9.0R3.1 (build 51667)[9.0.3-51667(3011)]	[Download]
Pulse Application Launcher Installer (MacOS)	This setup application installs all Pulse Application Launcher components.	version: 9.0R3.1 (build 51667)[9.0.3-51667(3011)]	[Download]

Testing Network Connectivity

You can use the admin console to test network connectivity to all the servers with which the system is configured to communicate, for example network services or AAA servers.

To test network connectivity:

1. Select **Maintenance > System > Platform** to display the system maintenance platform page.
2. Click **Test Connectivity**.

The screenshot displays the 'System Maintenance > Platform' interface. At the top, there are navigation tabs: 'Platform' (selected), 'Upgrade/Downgrade', 'Change Personality', 'Options', and 'Installers'. Below the tabs, a server icon is shown next to system details: Hostname: localhost2, Model: PSA-3000, Serial Number: 0312122015100079, Uptime: 10 days, 1 hour, 47 minutes, 59 seconds, Current version: 5.3R5 (build 38279), and Rollback version: 5.2R7 (build 36297). Under 'Node operations', there are buttons for 'Restart Services', 'Reboot...', 'Shut Down...', and 'Rollback...'. The 'Connectivity' section includes a 'Test Connectivity' button and a description: 'This will ping various configured servers to test the device's connectivity'. Below this is a 'Hardware Status' section with a 'Fan Status' table:

Fan	Status
2	●

The bottom section, 'Server connectivity results', lists several ping test outcomes:

- Destination host 10.96.64.1 used as Gateway Address is responding.
- Destination host 10.204.91.73 used as DNS Server is responding.
- Destination host eqe used as LDAP Server is not responding to icmp ping requests.
- Destination host apidev-as.avmdm.com used as MDM Server is responding.
- Destination host m-mobilizon.net used as MDM Server is not responding to icmp ping requests.

Logging and Monitoring

Logging Overview

Ivanti Policy Secure(IPS) provides logging and monitoring capabilities to help you track events and user activities. The system generates event logs related to system performance, administrator actions, network communications, access management framework results, user sessions, and so forth.

The available logs, includes:

- **Event Logs-** This file contains a variety of system events, such as session timeouts, systems errors and warnings, server restart notifications and connectivity requests.
- **User Access Logs-** This file contains information about when the user access the appliance, time, number of simultaneous users, user sign-ins and sign-outs.
- **Admin Access Logs-** This file contains administration information, including administrator changes to user, system and network settings, such as changes to session timeouts, license changes and so on.
- **Sensor Log-** This file contains information related to IDP sensor.

The system supports the following log collection methods:

- Local log collector and log viewer.
- Reporting to syslog servers.
- Reporting to SNMP servers.

The following table describes the event log severity levels.

Severity Level	Description
Critical	The system cannot serve user and administrator requests or loses functionality to a majority of subsystems.
Major	The system loses functionality in one or more subsystems, but users can still access the system for other access mechanisms.

Severity Level	Description
Minor	The system encounters an error that does not correspond to a major failure in a subsystem. Minor events generally correspond to individual request failures.
Info	The system writes an informational event to the log when a user makes a request or when an administrator makes a modification.

In addition to managing system logs, you can use the admin console to configure collection of client-side logs, including Host Checker logs.

Displaying System Logs

This topic describes how to display local system logs.

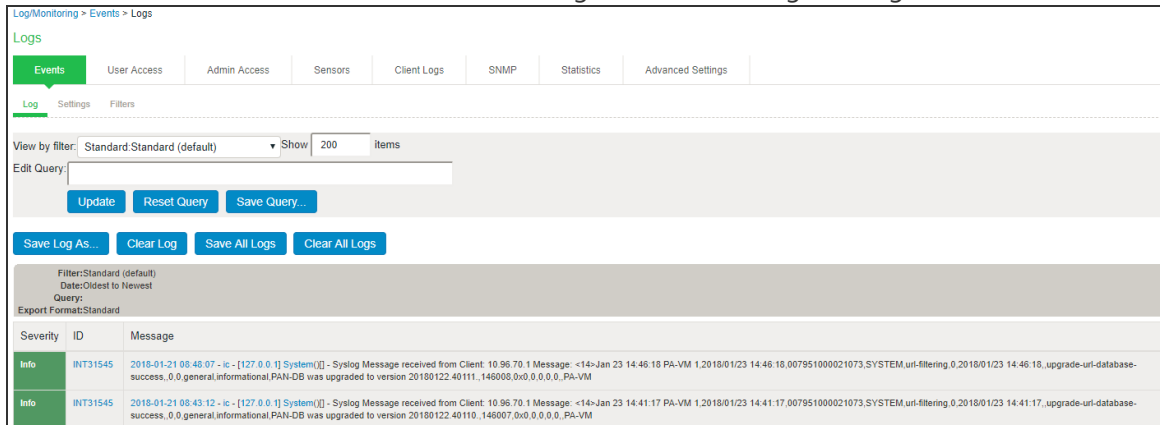
Displaying Events Logs


The Events logs include system events, such as session timeouts, system errors and warnings, requests to check server connectivity, and system restart notifications. The local log viewer displays the most recent 5000 log messages (the display limit).


To display Events logs:

1. Select **System > Log/Monitoring**.
2. Click the **Events** tab.
3. Click the **Log** tab to display the log page.

4. Use the features described in table to examine log records or manage the log collection.



Controls	Description
Filter	<p>Select a filter format. Any custom filter formats and the following predefined filter formats are available:</p> <ul style="list-style-type: none"> Standard (default)—This log filter format logs the date, time, node, source IP address, user, realm, event ID, and message. WELF—This customized WebTrends Enhanced Log Format (WELF) filter combines the standard WELF format with information about the system realms, roles, and messages. WELF-SRC-2.0-Access Report—This filter adds access queries to the customized WELF filter. You can use this filter with NetIQ’s SRC to generate reports on user access methods. <hr/> <p> Format filters change only the data displayed (or columns exported), and do not affect the log data that has been collected.</p> <hr/>
Query	<p>In the log display, several fields are hyperlinks. The hyperlinks function as dynamic queries on the local log collection. For example, if you click the log ID, the date, or an IP address or username, the log viewer queries the log collection for records that match the value you clicked, and redisplay the log collection. You can apply additional query filters by clicking additional hyperlinked values, essentially creating a Boolean AND query (for example, date AND IP address). Use the Reset Query button to clear the query filters and redisplay the unfiltered log collection.</p>

Controls	Description
	<p>Use the Save Query button to save the dynamic log query as a custom filter. When you click the Save Query button, the system displays the Filters tab displays with the Query field prepopulated with the variables you selected from the log.</p> <hr/> <p> Query filters change only the display (or rows exported), and do not affect the log data that has been collected.</p> <hr/>
Save Log As	<p>Save the local log collection to a file. We recommend you retain the system generated log name, which follows a consistent convention: pulsesecure.logtype.nodename.log.</p> <p>The local log viewer displays the most recent 5000 log messages (the display limit). If the current log file contains fewer than 5000 log messages, older log messages from the backup log file are displayed, up to a total of 5000 log messages. This makes the log files appear as one, even though they are stored separately.</p> <p>When you save the log messages or use the FTP archive function, the backup log file is appended to the current log file, and is then downloaded as one log file. If the log files are not archived or saved by the time they are rolled over again, the oldest log messages (saved in the backup log file) are lost.</p>
Clear Log	<p>Clear the local log and log.old file.</p> <p>When you clear the local log, events recorded by the syslog server are not affected. Subsequent events are recorded in a new local log file.</p>
Save All Logs	<p>The Save All Logs button appears on the Events, User Access, Admin Access, and Sensors tabs. When you click Save All Logs, the system generates a file that includes event, user access, admin access, sensor logs, and XML data for all of the system statistics and graphs shown on the Status > Overview page. After you click Save All Logs, you are prompted to download a file named pulsesecurelogs-graphs.tar.gz to your local host.</p>
Clear All Logs	<p>The Clear All Logs button appears on the Events, User Access, Admin Access, and Sensors tabs. It clears event, user access, admin access, sensor logs, and XML data for all of the system statistics and graphs shown on the Status > Overview page. When you clear the local log, events recorded by the syslog server are not affected. Subsequent events are recorded in a new local log file.</p>

Displaying User Access Logs

The User Access logs include information about user access, such as the number of simultaneous users at each one hour interval (logged on the hour) and user sign-ins and sign-outs. The local log viewer displays the most recent 5000 log messages (the display limit).

To display User Access logs:

1. Select **System > Log/Monitoring**.
2. Click the **User Access** tab.
3. Click the **Log** tab.

Displaying Admin Access Logs

The Admin Access logs include information about administrator actions, such as administrator changes to user, system, and network settings. It includes a log entry whenever an administrator signs in, signs out, or changes licenses on the appliance. The local log viewer displays the most recent 5000 log messages (the display limit).

To display Admin Access logs:

1. Select **System > Log/Monitoring**.
2. Click the **Admin Access** tab.
3. Click the **Log** tab.
4. Use the features to examine log records or manage the log collection.

Displaying Sensor Logs

The Sensor logs include information related to communication with an IDP sensor if you have deployed a coordinated threat control solution. The local log viewer displays the most recent 5000 log messages (the display limit).

To display Sensor logs:

1. Select **System > Log/Monitoring**.
2. Click the **Sensor** tab.

3. Click the **Log** tab.
4. Use the features to examine log records or manage the log collection.

Configuring Log Events Settings

The log type has its own settings that allow you to specify which events are logged, the maximum file size, and whether to log events to system log server in addition to logging them locally.

To configure log event categories:

1. Select **System > Log/Monitoring**.
2. Click the **Settings** tab to display the configuration page.
3. Complete the configuration as described below.
4. Save the configuration.



To configure log events for each local log category, you must perform this procedure on each local log tab: Events, User Access, Admin Access, and Sensors.

Settings	Guidelines
Maximum Log Size	
Max Log Size	<p>Specify the maximum size of the local log. The default is 200 MB. The maximum is 500 MB. The default is a good choice for logs formatted with the Standard format. If you use a more verbose format, such as WELF, specify a larger value. When the local log reaches the maximum log size, the current data is rolled over to a backup log file. A new, empty, file is then created for all subsequent (new) log messages. The log viewer displays the most recent 5000 log messages (the display limit). If the current log file contains fewer than 5000 log messages, older log messages from the backup log file can be displayed, up to a total of 5000 log messages. This makes the log files appear as one, even though they are stored separately.</p> <p>When you save the log messages or use the FTP archive function, the backup log file is appended to the current log file and is then downloaded as one log file. If the log files are not archived or saved by the time they are rolled over again, the oldest log messages (saved in the backup log file) are lost.</p>

Settings	Guidelines
Archiving	Click the Archiving link to display the configuration page for Archiving jobs, including log archiving.
Select Events to Log – Events Tab	
Connection Requests	Log events related to connection requests.
System Status	Log events related to changes in system status.
System Errors	Log events related to system errors.
Enforcer Events	Log events related to Infranet Enforcer communication.
Enforcer Command Trace	Log events related to Infranet Enforcer command execution.
Statistics	Log user access statistics reported on the System > Log/Monitoring > Statistics tab. If you unselect the Statistics option, the statistics are not written to the log file, but are still reported on the statistics page.
Performance	Log events related to performance, such as CPU utilization.
License Protocol Events	Log events related to licensing.
IF-MAP Server Trace	Log events related to IF-MAP.
RADIUS Statistics	Logs events related to RADIUS.
Select Events to Log – User Access Tab	
Login/log out	Log events related to sign in and sign out.
User Settings	Log events related to changes to user settings.
Client Certificate	Log events related to certificate security.
Enforcer Deny Messages	Log events related to Infranet Enforcer.
IF-MAP Client User Messages	Log events related to IF-MAP.

Settings	Guidelines
RADIUS Accounting Messages	Log events related to RADIUS.
Endpoint Heartbeat Messages	Log events related to endpoint heartbeat messages.
Pulse Client Messages	Log events related to Pulse clients.
Select Events to Log – Admin Access Tab	
Administrator changes	Log events related to configuration changes.
Administrator log ins	Log events related to administrator access.
License changes	Log events related to licensing.
Select Events to Log – Sensor Tab	
None	If you have configured communication with an IDP sensor for coordinated threat control, communication between the network nodes is logged. There is no way to select less than the whole set of sensor event logs.

Log Filtering

Ivanti Policy Secure(IPS) allows you to filter and format the data in your events, user access, and administrator access log files. When you filter log files, IPS displays only those messages specified within the filter query. For example, you can create a query that logs only entries for a particular range of IP addresses, or users who are signed into a specific realm. This topic describes how to use log filters.

Creating a Custom Log Collection Filter

If desired, you can create custom log collection filters to change the records displayed or exported. For example, it is common to see administrators use a filter for RADIUS accounting logs. This filter allows only the accounting log message, and it puts the entire message in a comma separated list. The order of the filtered message is: Date, Time, User, Realm, "List of Roles", NAS-ID, Acct-Status, Auth-Type, Attr-Value1, Attr-Value2, Attr-Value3.

Accounting attribute messages are different from authentication attribute messages in that the attribute name is not printed in the log message, but a comma is inserted for every attribute to be logged, even if it is not present.

To create a custom log collection filter:

1. Select **System > Log/Monitoring**.
2. Click the **Events** tab.
3. Click the **Filter** tab.
4. Click **New Filter** to display the configuration page.
5. Complete the configuration as described in table.
6. Save the configuration.

Settings	Guidelines
Filter Name	Specify a name that is helpful to you and other administrators in understanding usage for your customer filter.
Make default	Make the filter the default on syslog and archiving configuration pages.
Query	
Start Date	Enter a start date. Click Earliest Date to write all logs from the first available date stored in the log file.
End Date	Enter an end date. Click Latest Date to write all logs up to the last available date stored in the log file.
Query	Use the Filter Variables Dictionary to insert query expressions in the Query box. Enclose the query value in single quotes.

Settings	Guidelines
	For example, insert the query expression sourceip= . Then complete the expression by adding the value '192.168.0.1' .
Export Format	Select an export format: <ul style="list-style-type: none"> • Standard (default)—This log filter format logs the date, time, node, source IP address, user, realm, event ID, and message. • WELF—This customized WebTrends Enhanced Log Format (WELF) filter combines the standard WELF format with information about the system realms, roles, and messages. • Custom—Use the Standard as a template for your custom selection of columns to be included in exports (when log collections are saved to files).



Log query filters change only the data displayed (or rows exported). Log format filters change only the data displayed (or columns exported). Use of filters does not affect the log data that has been collected.

Reviewing the Configuration of Predefined Log Format Filters

To view the configuration of predefined log format filters:

1. Select **System > Log/Monitoring**.
2. Click the **Events** tab.
3. Click the **Filter** tab to display the log filters page.
4. Click the hyperlinked name of the filter to display its configuration page. You cannot edit the predefined filter named Standard, but you may edit the predefined WELF filters and any other custom filters that appear in the list.

Example: Using the Source IP Address Filter

When drilling into logs to verify behavior or troubleshoot an issue with a dual-stack device, it is helpful to redisplay the log collection filtered on the IP address.

To filter on an IP address:

1. Select **System > Log/Monitoring**.
2. Create the filter:
3. Select **User Access** and then **Filter**.
4. Define the filter expression, name the filter, and click **Save**. In this example, we create a filter based on source IP address and name it IPv6_Address_Filter:Standard.
5. Use the filter:
6. Select **Logs** to display the user logs table.
7. Under View by filter, select **IPv6_Address_Filter:Standard**.
8. If desired, under Edit Query, edit the value of the **sourceip= variable expression to filter on different source IP** addresses.
9. Click **Update** to apply the filter and redisplay the log collection.

Displaying User Access Statistics

Every hour, the system logs the peak count of Web users in the previous hour. It displays the hourly counts for the past week on the Statistics page. It writes the report to the system log once a week.

To display user statistics:

1. In the admin console, select **System > Log/Monitoring**.
2. Click the **Statistics** tab to display the page.
3. Scroll the page to view the data.



Upgrading software clears all statistics. If you configure the system to log statistics hourly, however, older statistics are still available in the log file after an upgrade.

Monitoring using SNMP


You can use a third-party SNMP manager, such as HP OpenView, to monitor IPS system health. IPS supports SNMP version 2 (v2) and SNMPv3. IPS implements a private MIB, and defines its own traps. Download the IPS MIB file and specify the appropriate information to receive the traps.


To configure the SNMP agent:

1. Select **System > Log/Monitoring**.
2. Click the **SNMP** tab to display the SNMP configuration page.
3. Complete the configuration as described in table.
4. Save the configuration.

Keep the following configuration tips in mind when you configure your SNMP manager to listen for this SNMP agent:

Settings	Guidelines
MIB File	Use the Ivanti MIB file link to download the device management information base MIB file. You add this file to your SNMP manager configuration.
SNMP Version	Select your SNMP server version: v2c v3
Agent Properties	
SNMP Queries	Select to support SNMP queries.
SNMP Traps	Select to send SNMP traps.
System Name	Specify a system name.
System Location	Specify a location.
System Contact	Specify a system contact.
Community String	<ul style="list-style-type: none"> · Required only for SNMPv2c. · To query the system, your network management station must send it the community string. · To stop the SNMP system, clear the community field.
SNMPv3 Configuration	

Settings	Guidelines				
Username	Specify the SNMPv3 username. The User-Based Security Model (USM) is the default Security Module for SNMPv3. The system supports only one user at a time to be registered with an SNMP engine. Editing the SNMPv3 user attributes overwrite any already registered SNMPv3 user. The SNMPv3 user must have read-only access on all MIBs supported by the system. SNMPv3 user configuration attributes can also be used for SNMP traps.				
Security Level	Selection	Auth Protocol	Auth Password	Priv Protocol	Priv Password
	No Auth, NoPriv	—	—	—	—
	Auth, NoPriv	Select MD5 (HMAC-MD5-96) or SHA (HMAC-SHA-96).	Enter an authentication password. The password can contain any ASCII characters and must be at least 8 characters in length.	—	—
	Auth, Priv	Select MD5 (HMAC-MD5-96) or SHA (HMAC-SHA-96).	Enter an authentication password. The password can contain any ASCII characters and must be at least 8 characters in length.	Select either CBC-DES or CFB-AES-128.	Enter a privacy password. The password can contain any ASCII characters and must be at least 8 characters in length.
Trap Thresholds	 Setting a threshold value to 0 disables that respective trap.				

Settings	Guidelines
Check Frequency	Specify the frequency in seconds for sending traps. The default is 180 seconds.
Log Capacity	Specify the percent of log space used. The default is 90%.
Users	Specify the percent of user capacity used. The default is 100%.
Physical Memory	Specify the percent of physical memory used. The default is 0 (not reported).
Swap Memory (Virtual Memory)	<p><u>Specify the percent of swap memory used. The default is 0 (not reported).</u></p> <p> We recommend you monitor swap memory to alert you to potential memory issues. The threshold for traps for physical memory usage might be reached even if the system is not experiencing any difficulties.</p>
Disk	Specify the percent of disk utilization. The default is 80%.
CPU	Specify the percent of CPU utilization. The default is 0 (not reported).
Meeting Users	Specify the percent of meeting users. The default is 100%.
Optional Traps	
Critical Log Events	Send traps when the system logs critical events.
Major Log Events	Send traps when the system logs major events.
Save SNMP Settings?	Click Save Changes to update the SNMP agent configuration. The page is refreshed and displays the SNMP engine ID. If the configuration is changed to move from SNMP v2c to SNMP v3, the system generates and displays two engine IDs.
SNMP Servers	
Hostname / IP address	Specify the hostname or IP address for the SNMP servers to which the system will send any traps it generates.
Port	Specify the port for the SNMP server. Typically, SNMP uses port 162.
Community	Specify the community string (if necessary).

- Add the Ivanti MIB file to the SNMP manager configuration.
- If using SNMPv2c, the community string configuration for the SNMP manager and SNMP agent must match.
- If using SNMPv3, the SNMPv3 user configuration for the SNMP manager and the SNMP agent must match.
- If using SNMPv3, you must specify the Authoritative Engine ID for SNMPv3 traps that was generated when you saved the SNMP agent configuration.

The table below is a reference of MIB objects for the system.

Object	Description
logFullPercent	Returns the percentage of available file size filled by the current log as a parameter of the logNearlyFull trap.
signedInWebUsers	Returns the number of users signed in through a Web browser.
signedInMailUsers	Returns the number of users signed in to the e-mail client.
blockedIP	Returns the IP address—blocked due to consecutive failed log in attempts—sent by the iveTooManyFailedLoginAttempts trap. The system adds the blocked IP address to the blockedIPList table.
authServerName	Returns the name of an external authentication server sent by the externalAuthServerUnreachable trap.
productName	Returns the licensed product name.
productVersion	Returns the software version.
fileName	Returns the file name sent by the archiveFileTransferFailed trap.
meetingUserCount	Returns the number of concurrent meeting users sent by the meetingUserLimit trap.

Object	Description
iveCpuUtil	Returns the percentage of CPU used during the interval between two SNMP polls. This value is calculated by dividing the amount of CPU used by the amount of CPU available during the current and previous SNMP polls. If no previous poll is available, the calculation is based on the interval between the current poll and system boot.
iveMemoryUtil	Returns the percentage of memory utilized by the system at the time of an SNMP poll. The system calculates this value by dividing the number of used memory pages by the number of available memory pages.
iveConcurrentUsers	Returns the total number of users logged in.
clusterConcurrentUsers	Returns the total number of users logged in for the cluster.
iveTotalHits	Returns the total number of hits to the system since last reboot. Includes total values from iveFileHits, iveAppletHits, meetingHits, and iveWebHits.
iveFileHits	Returns the total number of file hits to the system since last reboot. Incremented by the Web server with each GET/POST corresponding to a file browser request.
iveWebHits	Returns the total number of hits by means of the Web interface since last reboot. Incremented by the Web server for each http request received by the system, excluding file hits, applet hits, and meeting hits.
iveAppletHits	Returns the total number of applet hits to the system since last reboot. Incremented by the Web server for each GET request for a Java applet.
ivetermHits	Returns the total number of terminal hits to the system since last reboot.

Object	Description
logName	Returns the name of the log (admin/user/event) for the logNearlyFull and iveLogFull traps.
iveSwapUtil	Returns the percentage of swap memory pages used by the system at the time of an SNMP poll. The system calculates this value by dividing the number of swap memory pages used, by the number of available swap memory pages.
diskFullPercent	Returns the percentage of disk space used in the system for the iveDiskNearlyFull trap. The system calculates this value by dividing the number of used disk space blocks by the number of total disk space blocks.
blockedIPList	Returns a table with the 10 most recently blocked IP addresses. The blockedIP MIB adds blocked IP addresses to this table
ipEntry	An entry in the blockedListIP table containing a blocked IP address and its index (see IPEntry).
IPEntry	The index (ipIndex) and IP address (ipValue) for an entry in the blockedIPList table.
ipIndex	Returns the index for the blockedIPList table.
ipValue	A blocked IP address entry in the blockedIPList table.
logID	Returns the unique ID of the log message sent by the logMessageTrap trap.
logType	Returns a string sent by the logMessageTrap trap stating whether a log message is major or critical.
logDescription	Returns a string sent by the logMessageTrap trap stating whether a log message is major or critical.
Name	Returns the name of a virtual system.
ocspResponderURL	Returns the name of an OCSP responder.
fanDescription	Returns the status of the system fans.

Object	Description
psDescription	Returns the status of the system power supplies.
raidDescription	Returns the status of the system RAID device.
iveLogNearlyFull	<p>The log file (system, user access, or administrator access) specified by the logName parameter is nearly full. When this trap is sent, the logFullPercent (%of log file full) parameter is also sent. You can configure this trap to be sent at any percentage. To disable this trap, set the Log Capacity trap threshold to 0%. The trap's default value is 90%.</p> <p>When SNMP traps are enabled, the iveLogNearlyFull and iveLogFull traps are sent when the log files are 90% full and 100% full respectively, even if the threshold is set to 0 (disabled).</p>
iveLogFull	<p>The log file (system, user access, or administrator access) specified by the logName parameter is completely full.</p> <p>NOTE: When SNMP traps are enabled, the iveLogNearlyFull and iveLogFull traps are sent when the log files are 90% full and 100% full respectively, even if the threshold is set to 0 (disabled).</p>
iveMaxConcurrentUsersSignedIn	Maximum number or allowed concurrent users are currently signed in. You can configure this trap to be sent at any percentage. To disable this trap, set the Users trap threshold to 0%. The trap's default value is 100%.
iveTooManyFailedLoginAttempts	<p>A user with a specific IP address has too many failed sign-in attempts. Triggered when a user fails to authenticate according to the settings for the Lockout options on the Security Options tab.</p> <p>When the system triggers this trap, the system also triggers the blockedIP (source IP of log in attempts) parameter.</p>
externalAuthServerUnreachable	An external authentication server is not responding to authentication requests.

Object	Description
	When the system sends this trap, it also sends the authServerName (name of unreachable server) parameter.
iveStart	The system has just been turned on.
iveShutdown	The system has just been shut down.
iveReboot	The system has just been rebooted.
archiveServerUnreachable	The system is unable to reach the configured archive server.
archiveServerLoginFailed	The system is unable to log into the configured archive server.
archiveFileTransferFailed	The system is unable to successfully transfer files to the configured archive server. When the system sends this trap, it also sends the fileName parameter.
iveRestart	Supplies notification that the system has restarted according to the administrator's instruction.
iveDiskNearlyFull	Supplies notification that the system disk drive is nearly full. When the system sends this trap, it also sends the diskFullPercent parameter. You can configure this trap to be sent at any percentage. To disable this trap, set the Disk trap threshold to 0%. This trap's default value is 80%.
iveDiskFull	Supplies notification that the system disk drive is full.
logMessageTrap	The trap generated from a log message. When the system sends this trap, it also sends the logID, logType, and logDescription parameters.
memUtilNotify	Supplies notification that the system has met the configured threshold for memory utilization. To disable this trap, set the Physical Memory trap threshold to 0. The threshold is 0%, by default.

Object	Description
cpuUtilNotify	Supplies notification that the system has met the configured threshold for CPU utilization. To disable this trap, set the CPU trap threshold to 0. The threshold is 0%, by default.
swapUtilNotify	Supplies notification that the system has met the configured threshold for swap file memory utilization. To disable this trap, set the Swap Memory trap threshold to 0. The threshold is 0%, by default.
iveFanNotify	Supplies notification that the status of the fans has changed.
ivePowerSupplyNotify	Supplies notification that the status of the power supplies has changed.
iveRaidNotify	Supplies notification that the status of the RAID device has changed.
iveNetExternalInterfaceDownTrap (nicEvent)	Supplies the type of event that brought down the external interface. The nicEvent parameter can contain values of "external" for an external event and "admin" for an administrative action.
iveNetInternalInterfaceDownTrap (nicEvent)	Supplies the type of event that brought down the internal interface. The nicEvent parameter can contain values of "external" for an external event and "admin" for an administrative action.
iveClusterDisableNodeTrap (clusterName,nodeList)	Supplies the name of the cluster that contains disabled nodes, as well as a string containing the names of all disabled nodes. Node names are separated by white space in the string.
iveClusterChangedVIPTrap(vipType, currentVIP, newVIP)	Supplies the status of a virtual IP for the cluster. The vipType indicates whether the changed VIP was external or internal. The currentVIP contains the VIP prior to the change, and newVIP contains the VIP after the change.

Object	Description
iveNetManagementInterfaceDownTrap (nicEvent)	Supplies the type of event that brought down the management port. The nicEvent parameter can contain values of "external" for an external event and "admin" for an administrative action.
iveClusterDelete(nodeName)	Supplies the name of the node on which the cluster delete event was initiated.
pclsRemainingGracePeriod	Number of days remaining in grace period for contacting PCLS
iveMaxConcurrentUsersLicenseCapacity	Total licensed concurrent users capacity

Configuring an External Syslog Server

Ivanti Policy Secure(IPS) allows you to send the log data to an external syslog server. You should use syslog if your enterprise has any long-term record-keeping or accounting requirements.


To configure reporting to a syslog server:

1. Select **System > Log/Monitoring**.
2. Click the **Settings** tab.
3. Specify the maximum log size and select the events to be logged.
4. Specify the server configuration as described below and click Add. You can specify multiple syslog servers.
5. Save the configuration.



To enable syslog reporting for each local log category, you must perform this procedure on each local log tab: Events, User Access, Admin Access, and Sensors.

Settings	Guidelines
Server name/IP	Specify the fully qualified domain name or IPv4/IPv6 address for the syslog server. NOTE: If you select TLS from the Type list, the server name must match the CN in the subjectDN in the certificate obtained from the server.

Settings	Guidelines
Facility	<p>Select a syslog server facility level (LOCAL0-LOCAL7).</p> <p>Your syslog server must accept messages with the following settings: facility = LOG_USER and level = LOG_INFO.</p>
Type	<p>Select the connection type to the syslog server. You can select:</p> <ul style="list-style-type: none"> • UDP (User Datagram Protocol) - A simple non-secure transport model. • TCP (Transmission Control Protocol) - A core protocol of the Internet Protocol suite (IP), but lacks strong security. • TLS (Transport Layer Security) - Uses cryptographic protocols to provide a secure communication.
Client Certificate	<p>(optional) If you select TLS from the Type menu and your remote syslog server requires client certificates, select the installed client certificate to use to authenticate to the syslog server. Client certificates are defined in the Configuration > Certificates > Client Auth Certificates page. Client certificates must be installed on the device before they can be used.</p> <hr/> <p> There is no fallback if a connection type fails.</p> <hr/>
Filter	<p>Select a filter format. Any custom filter format and the following predefined filter formats are available:</p> <ul style="list-style-type: none"> • Standard (default)—This log filter format logs the date, time, node, source IP address, user, realm, event ID, and message. • WELF—This customized WebTrends Enhanced Log Format (WELF) filter combines the standard WELF format with information about the system realms, roles, and messages. • WELF-SRC-2.0-Access Report—This filter adds access queries to the customized WELF filter. You can use this filter with NetIQ's SRC to generate reports on user access methods.

Configuring Advanced Settings

This option helps to configure fault tolerance on each configured TCP and TLS syslog server available. Fault tolerance is supported only for TCP and TLS syslog servers. UDP syslog servers cannot be configured for fault-tolerance. This functionality helps the syslog server to recover the logs lost during a disconnect. The administrator can configure fault-tolerance on syslog servers by enabling this option from the admin UI. IPS/ICS reads the lost pending logs during a disconnect from the log disk and transports them to the syslog server on a reconnect. Fault tolerance is supported only for the syslog servers configured under the following log-types:

- Events
- User Access
- Admin Access



Fault tolerance is node-specific. In case of clusters, the setting needs to be enabled/disabled by logging into each of the cluster members.

To configure advance settings to a TCP and TLS syslog server:

1. Select **System > Log/Monitoring**.
2. Click the **Advance Settings** tab to display the configuration page.
3. Complete the configuration as described in table.
4. Save the configuration.



This feature is limited to configuring fault tolerance settings of an existing syslog server; and cannot be used to create or delete a new syslog server.

Settings	Guidelines
Syslog Server Fault Tolerance	
Syslog Server	Lists the existing Syslog servers.
Type	Specifies if the Syslog server is a TLS or TCP type.

Settings	Guidelines
Fault Tolerance	Tolerates the loss of network connection to a TCP/TLS syslog server for a brief period (maximum of 4 hours) by sending the logs missed during the disconnect time. Click the checkbox to enable this option. Fault-tolerance is disabled by default on any syslog server.

Enabling Client-Side Logging

Client-side logging is not enabled by default. You can enable client-side logging for Host Checker. IPS writes a client side log to endpoints when client side logging is enabled.

To enable client-side logging:

1. Select **System > Log/Monitoring**.
2. Click the **Client Logs** tab to display the configuration page.
3. Select the **Host Checker** option to enable client-side logging when Host Checker is run on the endpoint.
4. Save the configuration.

Displaying System Status

The System Status page is a dashboard of system version information, system capacity utilization, uptime, and summary user information. The System Status page is the “home” page that is displayed when you log into the admin console as an administrator.

To navigate to the System Status page from other admin console pages, select System > Status,

The table that follows describes the various options available.

Item	Description
1	Click the Critical Events link to display a new window with a table of the last 10 critical system events.
2	Click the Page Settings link to display a new window with the System Status Settings page.

Item	Description
3	Click the System Version Download Package link to download the software version running on the system. You might do this when you need to synchronize software on another node to the software version running on this system.
4	Click the System Date and Time Edit link to display the System Date and Time configuration page.
5	Click a System Capacity Utilization report Edit link to display a new window with controls to customize the appearance of the report graphs.
6	Click a System Capacity Utilization report Download link to download graph data in XML format.
7	Click an Enforcer Status link to navigate to its configuration page.

Item	Description
Licenses	
Max Licensed Users	Displays the maximum number of licensed users by supported platform type.
User Licenses Consumed	Displays how user licenses are being used. Pulse Client connections and agentless connections count as user licenses.
Total Users	
User Licenses	Displays the number of Pulse Client connections and agentless connections. These types of connections count as user licenses. The maximum number of licenses is the sum of the capacity provisioned by the licenses that have been added to the system.
MAC Address Users	Displays the number of connections through MAC Address authentication realms. This number is reported only if a MAC Address realm has been configured. These connections do not count as user licenses, and there is no maximum number of licenses set by rule.
RADIUS Users	Displays the number of RADIUS user connections. These connections do not count as user licenses, and there is no maximum number of licenses set by rule.

Item	Description
Total Signed-In Users	Displays the sum of user licenses in use. <ul style="list-style-type: none"> · User Licenses count · MAC Address Users count · RADIUS Users count

You can use this page to select the reports displayed on the System Status page, as well as data properties, such as the time dimension and refresh rate.

The following reports are available:

- **Concurrent Users**—Shows a count of users signed into the system. In clustered environments, the graph includes two lines. The first line displays the number of local users signed into the node selected from the list, and the second line displays the number of concurrent users signed into the entire cluster.
- **Hits per Second**—Shows a count of hits currently being processed by the system. In a clustered environment, you may select a node from the list to determine which node's data is displayed in the graph. The graph includes three lines: total number of hits, number of Web hits, and number of client/server hits.
- **CPU and Memory Usage**—Shows the percentage of the CPU and memory being used. In a clustered environment, you may select a node from the list to determine which node's data is displayed in the graph.
- **Throughput**—Shows the amount of data (in KB) being processed. In a clustered environment, you may select a node from the list to determine which node's data is displayed in the graph. The graph includes four lines: external in, external out, internal in, and internal out.
- **Connections**—Shows a count of concurrent SSL connections.
- **Rates**—Shows the rate of attempted log ins, successful log ins, and Host Checker updates.

Displaying Hardware Status

You can use the Maintenance > System > Platform page to display the hardware health status, including information about hard drives, fans, and power supplies.

To display hardware health status:

1. Select **Maintenance > System > Platform** to display the System Maintenance page.
2. Review the hardware status information described in table.

The below table lists the RAID status and hard drive status. Depending on your system, you may or may not see all these possible statuses.

Hardware Component	Status Message
Hard Disk Status	Displays a health statement for the device disk drive.
Fan Status	Displays a health statement for the device fan(s).
Power Supply	Displays a health statement for the device power supply.

RAID Status	Drive 1	Drive 2
Hard Disk RAID is operational	Active	Active
Hard Disk RAID is in single drive mode	Missing	Active
Hard Disk RAID is in single drive mode	Active	Missing
Hard Disk RAID has failed	Failed	Active
Hard Disk RAID has failed	Active	Failed
Hard Disk RAID is in the process of recovering	Active	Reconstructing
Hard Disk RAID is in the process of recovering	Reconstructing	Active
Hard Disk RAID is in the process of recovering	Active	Verifying
Hard Disk RAID is in the process of recovering	Verifying	Active
Hard Disk RAID status is unknown	Unknown	Active
Hard Disk RAID status is unknown	Active	Unknown
Hard Disk RAID status is unknown	Unknown	Unknown
Not available	n/a	n/a

Using Software RAID on PSA7000

 All hard disks are encrypted with AES128 using a random generated key.

This section describes the use of software RAID.

Overview of Software RAID

The PSA7000 device has two hard disks. However, there is no hardware RAID controller. In IPS 5.4R1, RAID functionality is enabled through the software RAID available in Linux. Software is used to create RAID devices in the RAID 1 layer. These individual disk partitions can also be used as regular partitions. All partitions, which include boot, root, data, var, tmp, swap, and so on are created out of the software RAID. Software RAID does not affect any of the other hardware models except PSA7000. It works the same way either with hardware RAID or no RAID at all.

Configuring RAID Controller

To configure a RAID controller on the PSA7000, disks are hot plugged on the PSA7000. Configuring RAID on the PSA7000 also involves some manual configuration steps in the admin console. RAID configuration is carried out by the following steps:

To remove a disk from the second slot in the system:

1. Select Menu option: **4. System Operations**
2. Select Menu option: **20. Manage RAID**
3. A prompt appears: **Are you sure you want to manage RAID? (y/n)**
4. Enter `y` for the prompt.
5. Choose Menu option: **2. Remove Disk2**. This will detach the disk in the second slot from software RAID.
6. Physically unplug the disk from the second slot.

To insert a disk to the second slot in the system:

1. Physically plug in the disk in the second slot.
2. Select Menu option: **4. System Operations**

3. Select Menu option: **20. Manage RAID**
4. A prompt appears: **Are you sure you want to manage RAID? (y/n)**
5. Enter `y` for the prompt.
6. Choose Menu option: **4. Add Disk2**. This will attach the disk in the second slot to the software RAID.

Checking RAID Statuses

To check the status of RAID and individual disks:

1. Go to **system > platform** page of the web interface.
2. Status of RAID and individual disks are displayed. The below table shows the hard disk status and the hard disk RAID status.

	Status	Guidelines
Hard Disk	Active	A disk that is present and part of RAID
	Inactive	A disk that is present but not part of RAID
	Missing	A disk that is removed.
Hard Disk RAID	Operation	Both disks are active and part of the software RAID
	Recovering	Both disks are active and syncing with each other
	Failed	Both disks are active but one of them is not part of RAID



In the single drive mode, only one disk is active. The other disk is either missing or inactive.

LCD Display

This section describes the addition of LCD to IPS devices.

Overview of adding LCD for IPS

The addition of a LCD screen allows field technicians to quickly gauge the health of the system without logging into the device. The buttons on the LCD panel allow navigation through the display menus. The directional buttons are used to access the menu modes and find device information. The LCD can display two line of text. The below figure shows the LCD screen with navigation buttons.



LCD display is available for the PSA-7000 platform model only.

Modes Supported by the LCD

The LCD supports two modes namely the display mode (default) and the menu mode. Pressing any button in the display mode will change the mode to menu mode. If a user presses the cancel button, the LCD immediately changes back to display mode and shows the appropriate state. The LCD remains in display mode. If the LCD is in menu mode and the user does not press any button for more than two minutes, then the LCD changes back to display mode. The below figure shows the two modes supported by the LCD

Display Mode

The display mode describes the current state of the system, such as normal state or error conditions (e.g., fan speed and overheat). It represents the default status. The LCD goes into display mode after boot-up is complete. In display mode, the LCD is either set to NORMAL or shows a label that describes an error condition. If all systems are functioning normally, then the LCD shows NORMAL. The second line in the NORMAL state is used to show whether the appliance is configured as part of a cluster. The valid states in the display mode are Clustering OFF and Clustering ON.

Detecting Error Conditions in Display Mode

If more than one error condition is detected, all error conditions will be displayed in sequence with a 2 second pause before switching to the next one. All error conditions need to be cleared before the status returns back to the NORMAL state. Error conditions include:

- Overheat
- Fan Failure
- RAID Errors

If there are any error conditions, they are automatically shown on the LCD screen when it is in the display mode. The types of errors displayed are: Fan Failures, CPU overheating and RAID errors. If there are multiple errors they would be displayed in the order with a two second pause between successive displays.

The error message is automatically cleared when the underlying error condition is resolved. For example: the CPU overheat message disappears when CPU temperature is lowered. The user can enter the Menu mode at any point, even if an error message is being displayed.

Menu Mode

The menu mode is activated when the user presses any button. A single press of the button changes to menu mode and loads the last selected menu selection.

To view information in the menu mode:

1. Press any button. This puts the LCD into menu mode.
2. Press the right and left arrows keys to obtain the available system configuration data.
3. View information starting with the Internal IP and moving in a clockwise direction.
4. The menu screens loop back in a cycle.
5. Press Cancel at any point to exit to display mode.



Any button, even cancel will put the user in the menu mode.

Displaying Active Users

You can use the Active Users page to display the system active users table and to perform administrative actions pertaining to active sessions.

The system active users table displays all users who have an active session (in contrast to the users tables that appear on the authentication server configuration pages, which display session records for active and inactive sessions that were authenticated by the particular authentication server).

If a user signs in and is placed in a VLAN without an IP address, the table does not display an IP address under Signed in IP.



If there is a NAT device between the user's computer and the Infranet Enforcer, the table displays both the NAT device's IP address and the endpoint's virtual source IP address under Signed in IP. For example, if the NAT device's IP address is 10.64.9.26, and the endpoint's virtual source IP address is 192.168.80.128, the following information is displayed under Signed in IP: 10.64.9.26 (192.168.80.128 behind NAT).

To display the system Active Users page:

1. Select **System > Status**.
2. Click the **Active Users** tab to display the system active users page.
3. Use the controls described in table below to perform administrative actions pertaining to active sessions.



Profiler publishes signed in IP address in Active users page only if RADIUS Accounting is disabled and signed in IP is not available for the user session.

Buttons	Administrative Actions
Update	<p>Refresh records displayed on the page:</p> <ul style="list-style-type: none"> • To refresh the page, click Update. • To display a specific user, enter the username in the Show Users Named box and click Update. If you do not know the exact username, use the asterisks (*) as a wildcard character. • To change the table size, enter a number in the Show N users box and click Update. <hr/> <p> To sort the table of currently signed-in users and administrators, click a column header.</p>
Delete Session	<p>Select the check box next to the appropriate names and then click Delete Session to immediately delete the session. The user is signed out by your action.</p>
Delete All Sessions	<p>Use this option to immediately delete all sessions. Users are signed out by your action.</p> <hr/> <p> If you want to sign out administrators, you must choose them individually and use the Delete Session button.</p>

Buttons	Administrative Actions
Refresh Roles	Manually evaluate all authentication policies, role-mapping rules, role restrictions, user roles, and resource policies for all currently signed-in users. Use this button if you make changes to an authentication policy, role-mapping rules, role restrictions, or resource policies and you want to immediately refresh the roles of all users.
Disable All Users	Sign out all end users who are currently signed-in and also prevent any other users from signing in. To allow users to sign in again after you disable all users, click Enable All Users.

Troubleshooting

Overview

You can use the admin console troubleshooting tools to investigate user access issues and system issues. The following tools are available through the Maintenance > Troubleshooting pages:

- Policy tracing—Diagnose user access issues.
- Debug logs—Work with PSGSC to diagnose system issues.
- RADIUS diagnostic log—Diagnose issues with IPS RADIUS server.
- tcpdump—Sniff packet headers to diagnose networking issues.
- Network troubleshooting commands—Use standard network commands, such as ping, traceroute, NSlookup, and other commands to diagnose networking issues.
- Kerberos debugging—Diagnose issues with Kerberos communication.
- System snapshots—Work with PSGSC to reproduce and diagnose system issues.
- Remote debugging—Enable PSGSC to access your system directly to help you diagnose system issues.

If the admin console is unavailable, you can use the serial port console to perform some troubleshooting operations, such as use ping and traceroute commands, view logs, create system snapshots, and perform configuration rollbacks and factory resets.

Policy Tracing

It is common to encounter a situation where the system denies a user access to the network or to resources, and the user logs a trouble ticket. You can use the policy tracing utility and log to determine whether the system is working as expected and properly restricting access, or whether the user configuration or policy configuration needs to be updated to enable access in the user's case.

To create a policy trace log:

1. Select **Maintenance > Troubleshooting > Policy Tracing** to display the configuration page.

Troubleshooting > User Session > Policy Tracing

Policy Tracing

[User Sessions](#) | [Monitoring](#) | [Tools](#) | [System Snapshot](#) | [Remote Debugging](#)

Policy Tracing

Record policy trace events for a given user under a given realm. Policy trace events determine policies applied on the user under the given realm. Enter the user, realm, and/or the source IP address, and check the events to be tracked. Events get logged from the time you *Start Recording*. In review.

Record Trace File

Status: Not Recording

User:

Source IP:

Realm:

Events to Log

Pre-Authentication
 Authentication
 Role Mapping
 IF-MAP

Sensor Event Policies

Infranet Enforcer Policies

 IPSec
 Auth Table Mapping
 Source Interface
 IP Address Pools

RADIUS Attributes Policies

Host Enforcer Policies

UAC Message Trace

Admission Control Policies

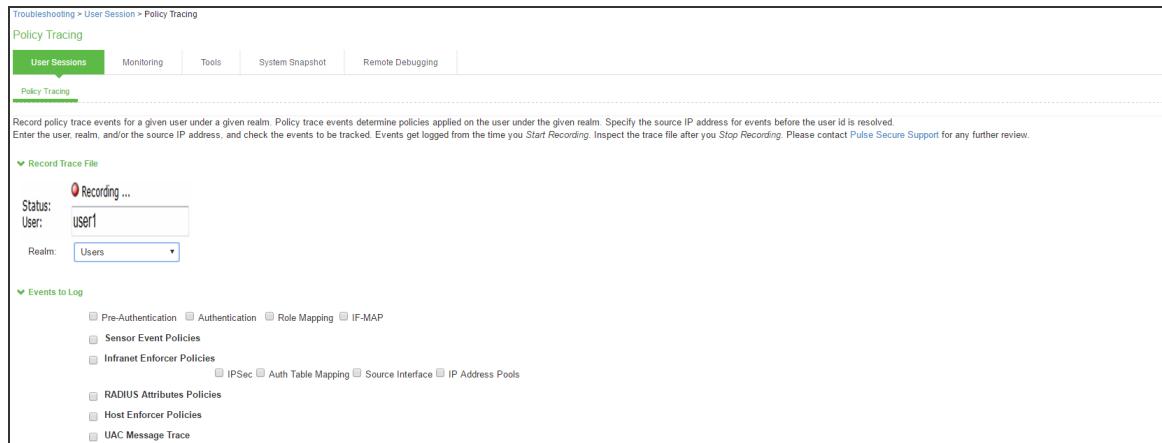
[Start Recording](#)
 [Delete Trace](#)
 [View Log >>](#)

2. Complete the configuration as described below.

Settings	Guidelines
Record Trace File	
User	Specify the username to trace. If you are tracing anonymous access, you can use the asterisks wildcard character (*) because you might not know the internal username the system assigns to the next anonymous session.
Source IP	Specify the source IP address if you know it. If you are able to provide the source IP address, the policy trace log can include events that occur before the user ID is entered into the system.
Realm	Select the realm to trace.
Events to Log	
Pre-Authentication	Logs events related to evaluation of realm rules.
Authentication	Logs events related to authentication.
Role Mapping	Logs events related to role mapping.
IF-MAP	Logs events related to IF-MAP queries related to the session.
Sensor Event Policies	Logs events related to sensor policies.
Infranet Enforcer Policies	Logs events related to Layer 3 Infranet Enforcer policies.
RADIUS Attributes Policies	Logs events related to Layer 2 802.1X access.
IPS Message Trace	Logs IPS messages.
Admission Control Policies	Logs events related to admission control policies.

3. Click **Start Recording**.

The following figure shows the policy tracing page with the recording indicator.



4. Initiate the action you want to trace, such as a user sign in.

5. Click **View Log** to display the policy trace results log.

6. Click **Stop Recording** when you have enough information.

Table describes options for managing the policy trace results log file.

Control	Guidelines
Delete Trace	Under Events to Log, click Delete Trace to clear the results displayed on this page.
Update	Specify a number of rows to display and click Update to change the number of rows that are displayed.
Save Log As	Click this button to save the trace results log to a file. This is useful particularly when you are working with the Ivanti Global Support Center to troubleshoot a case.
Clear Log	Click this button to clear the log file from the system.

Debug Logs

The Ivanti Global Support Center might direct you to create a debug log to assist them in helping you debug an issue with the system. The debug log is used only by PSGSC.

To use debug logging:

1. Select **Maintenance > Troubleshooting > Debug Log** to display the configuration page.
2. Complete the configuration as described below.
3. Click **Save Changes**. When you save changes with Debug Logging On selected, the system begins generating debug log entries.
4. Initiate the action you want to debug, such as a user sign in. You can reset the debug log file to restart debug logging if it takes you too long to initiate the action.
5. Click **Save Debug Log** to save the debug log to a file that you can send to PSGSC. You can clear the log after you have saved it to a file.
6. Unselect **Debug Logging On** and click **Save Changes** to turn off debug logging.

The screenshot shows the 'Debug Log' configuration page. At the top, there is a breadcrumb trail: 'Troubleshooting > Monitoring > Debug Log'. Below this, the page title is 'Debug Log'. A navigation bar contains tabs for 'User Sessions', 'Monitoring' (which is active and highlighted in green), 'Tools', 'System Snapshot', and 'Remote Debugging'. Underneath, there are sub-tabs: 'Debug Log' (active), 'Node Monitor', 'Cluster', 'Diagnostic Logs', and 'REST Monitor'. A row of four blue buttons is visible: 'Save Changes', 'Reset', 'Save Debug Log', and 'Clear Log...'. Below the buttons, a section titled 'Debug Log Settings' is expanded. It contains the following settings:

- Current Log Size: 3121019 bytes
- Debug Logging On:
- Max Debug Log Size: MB
- Debug Log Detail Level:
- Include logs:
- Process Names:
- Event Codes:

Settings	Guidelines
Current Log Size	Displays the size of the current log file. If it is large, use the controls to save, reset, or clear the log file.
Debug Logging On	Select to turn on debug logging.
Debug Log Size	Specify a maximum debug log file size. The default is 2 MB. The maximum is 250 MB.
Debug Log Detail Level	Specify the debug log detail level. Obtain this from PSGSC.
Include logs	Select this option to include system logs in the debug log file. Recommended.
Process Names	Specify the process name. Obtain this from PSGSC.
Event Codes	Specify the event code. Obtain this from PSGSC.

RADIUS Diagnostic Logs

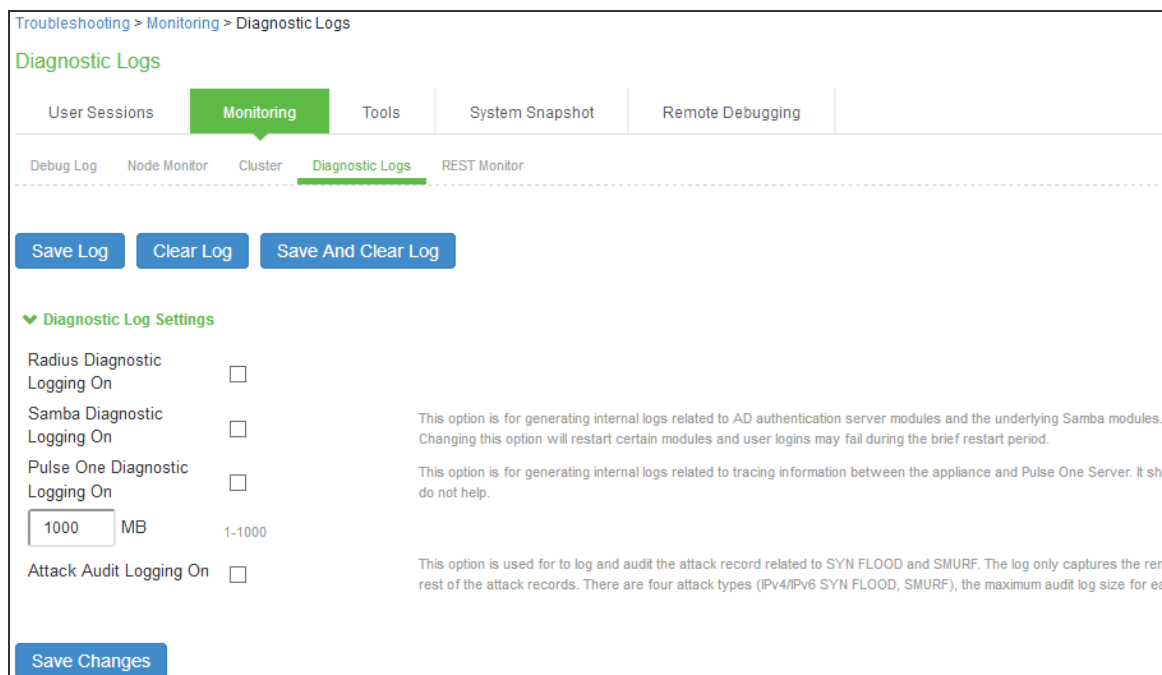
The RADIUS diagnostic log utility allows you to view trace and debug-level RADIUS messages. When RADIUS diagnostic logging is enabled, the diagnostic tool logs all requests that IPS receives from RADIUS clients. RADIUS requests initiated by IPS do not appear in the log.

Observe the following guidelines:

- Diagnostic logging affects system performance.
- All events that appear in the log have an ID code, and all messages in a thread are tagged with the same ID. This allows you to track individual log ins or log in attempts.
- Source IP addresses are represented as 127.0.0.1 (the loopback address).
- For Layer 2 connections, the calling station ID is the MAC address of the endpoint.
- Passwords are suppressed and do not appear in the logs.
- When the log fills up, logging stops. You can clear the log to restart logging.
- Raw traffic is not available in the log. To view raw traffic, use the tcpdump feature.

To use RADIUS diagnostic logging:

1. Select **Maintenance > Troubleshooting > Diagnostics Logs** to display the configuration page.
2. Complete the configuration as described below.
3. Click Save Changes. When you save changes with RADIUS Diagnostic Logging On selected, the system begins generating diagnostic log entries.
4. Initiate the action you want to debug, such as a user sign in. You can clear the debug log file to restart diagnostic logging if it takes you too long to initiate the action.
5. Manage the resulting log:
 - Click Save Log to save the log files in a zipped format.
 - Click Clear Log to remove previous logs and start diagnostic logging with a fresh file.
 - Click **Save And Clear Log** to save the diagnostic log to a file that you can send to PSGSC. The existing logs in the device will be cleared after saving.
6. Unselect RADIUS Diagnostic Logging On and click Save Changes to turn off diagnostic logging.



Settings	Guidelines
RADIUS Diagnostic Logging On	Specify the source IP address if you know it. If you are able to provide the source IP address, the policy trace log can include events that occur before the user ID is entered into the system.
Max Diagnostic Log Size	Specify a maximum logfile size. The default is 1000 MB.

Samba Diagnostic Logs

The Samba diagnostic log utility allows you to view trace and debug the samba troubleshooting messages on the new AD authentication server. When samba diagnostic logging is enabled, the internal logs related to AD authentication server is generated.

Observe the following guidelines:

- Diagnostic logging affects system performance.
- Must be used only when the admin UI error messages, event logs and admin logs are not very useful.
- Enabling/Disabling samba logs will restart certain modules and user log ins may fail during the restart.
- The default debug log setting will generate minimal logs. Enabling debug log with event AAA or AAA::samba along with this feature can generate more logs based on the debug log level.

Enabling samba logs will cause logs to be generated from all configured AD authentication servers. Logs from multiple AD servers are interleaved and can be identified by the header in each line of the logs.

To use samba diagnostic logging:

1. Select **Troubleshooting > Monitoring > Diagnostic Logs** to display the configuration page.
2. Complete the configuration as described below.
3. Click Save Changes. When you save changes with Samba Diagnostic Logging On selected, the system begins generating diagnostic log entries.
4. Initiate the action you want to debug, such as a user sign in.

5. Manage the resulting log:

- Click Save Log to save the log files in a zipped format.
- Click Clear Log to remove previous logs and start diagnostic logging with a fresh file.
- Click Save And Clear Log to save the diagnostic log to a file that you can send to PSGSC. The existing logs in the device will be cleared after saving.

6. Unselect Samba Diagnostic Logging On and click Save Changes to turn off diagnostic logging.

Settings	Guidelines
Samba Diagnostic Logging On	Select this option to generate logs related to AD server.
Max Diagnostic Log Size	Specify a maximum log file size. IPS <ul style="list-style-type: none"> • Default (MB)- 10 • Maximum (MB)-100

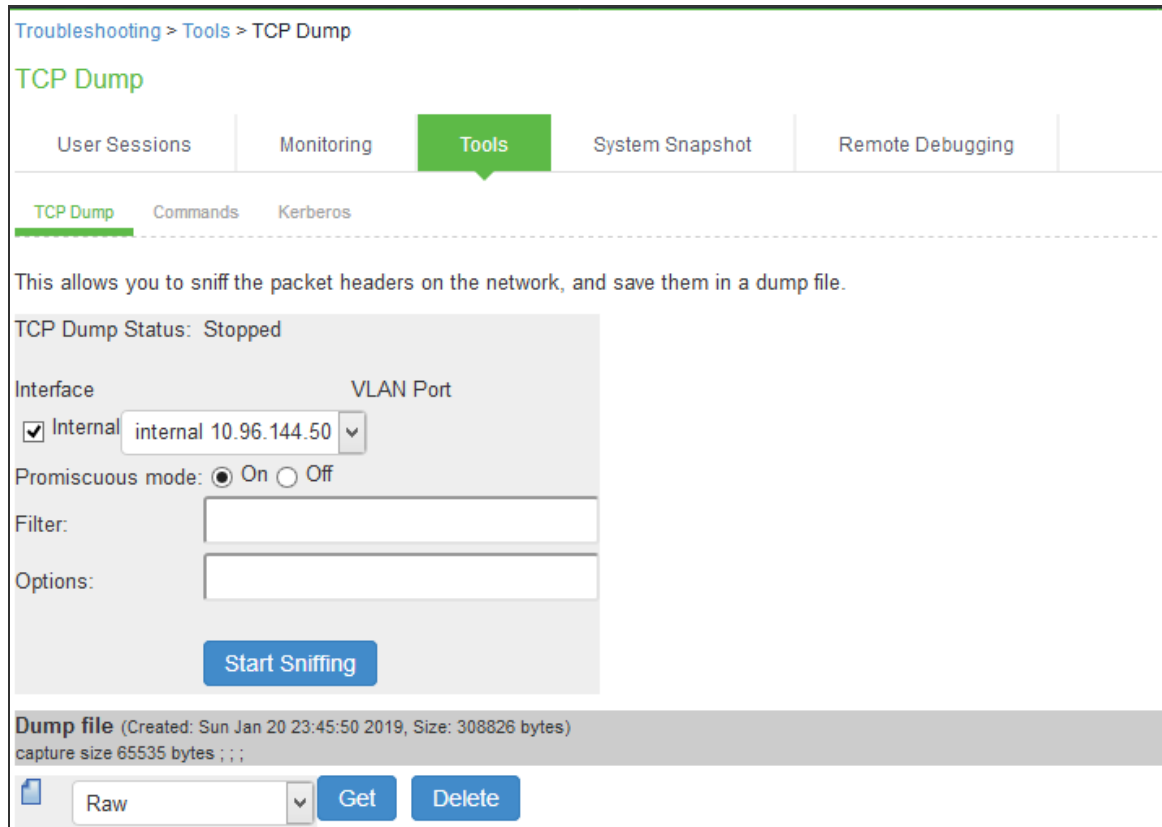
TCP Dump

This is a tool to sniff the packet, when you want to examine that the expected packet really reached a node. You can run the tcpdump utility to sniff the packet headers on the network and save them on a dump file.

To use tcpdump:

1. Select **Maintenance > Troubleshooting > TCP Dump** to display the configuration page.
2. Complete the configuration as described below.
3. Click **Start Sniffing** to start the tcpdump process.
4. Initiate the action you want to debug, such as a user sign in.
5. Click **Stop Sniffing** to write the tcpdump output to the screen.

- Click **Get** to save the output to a file, or click **Delete** to clear the output.



Settings	Guidelines
TCP Dump Status	Displays whether the utility is stopped or running.
Interface	Select the ports on which to sniff.
VLAN Port	Select the VLAN port.
Promiscuous mode	Select a promiscuous mode option.
Filter	Specify a filter expression. For information about TCP dump filter expressions, see the UNIX man page .

Settings	Guidelines	
	Example	Result
	tcp port 80	Sniffs packets on TCP port 80.
	port 80	Sniffs packets on TCP or UDP port 80.
	ip	Sniffs the IP protocol.
	tcp	Sniffs the TCP protocol.
	dst #.#.#.#	Sniffs the destination IP address specified, where #.#.#.# is a valid IP address.
	src #.#.#.#	Sniffs the source IP address specified, where #.#.#.# is a valid IP address.
	port 80 or port 443	Sniffs on port 80 or port 443.
	src #.#.#.# and dst #.#.#.#	Sniffs the source and destination IP addresses or hosts specified, where each #.#.#.# represents a valid IP address.
	tcp port 80 or port 443 and dst #.#.#.# and src #.#.#.#	This example shows how to specify multiple parameters to create a filter that sniffs on TCP port 80, or on TCP or UDP port 443, and on the destination and source ports, where each #.#.#.# represents a valid IP address.

Network Troubleshooting Commands

You can run common network troubleshooting commands such as arp, ping, ping6, traceroute, traceroute6, NSlookup, and AvgRTTs from the admin console. You can use these connectivity tools to see the network path from the system to a specified server. If a client can ping or traceroute to the access system, and the access system can ping the target server, any remote users should be able to access the server through the access system.

To run network troubleshooting commands:

1. Select **Maintenance > Troubleshooting > Commands** to display the configuration page.
2. Complete the configuration as described below.
3. Click **OK** to run the command and write the output to the screen.
4. Click **Clear** to clear the output.

The screenshot shows the 'Commands' configuration page in the admin console. The breadcrumb trail is 'Troubleshooting > Tools > Commands'. The page title is 'Commands'. There are four tabs: 'User Sessions', 'Monitoring', 'Tools' (which is selected and highlighted in green), and 'System Snapshot'. Below the tabs, there are three sub-tabs: 'TCP Dump', 'Commands' (which is selected and highlighted in green), and 'Kerberos'. The main configuration area contains the following fields and controls:


- Command:** A dropdown menu with 'Ping' selected.
- Target server:** An empty text input field.
- Interface:** A radio button selection with 'Internal Port' selected.
- VLAN Port:** A dropdown menu with 'internal 10.96.144.50' selected.
- Buttons:** Two blue buttons labeled 'OK' and 'Clear'.
- Output:** A section labeled 'Output:' with the text 'None' displayed below it.

Settings	Guidelines
Command	<p>Select a network troubleshooting command:</p> <ul style="list-style-type: none"> • Ping/Ping6-Use the ping command to verify that the system can connect to other systems on the network. In the event of a network failure between the local and remote nodes, you do not receive a reply from a pinged device. In that case, contact your LAN administrator for help. The ping command sends packets to a server and returns the server response, typically a set of statistics including the target server's IP address, the time spent sending packets and receiving the response, and other data. You can ping unicast or multicast addresses, and you must include the target server name in the request. Select ping to ping an IPv4 address or hostname. Select ping6 to ping an IPv6 address. We do not support DNS resolution for hosts with IPv6 addresses. Hence, ping6 does not support pings to hostnames. • Traceroute/Traceroute6-Use the traceroute command to discover the path that a packet takes from IPS to another host. Traceroute sends a packet to a destination server and receives an ICMP TIME_EXCEEDED response from each gateway along its path. The TIME_EXCEEDED responses and other data are recorded and displayed in the output, showing the path of the packet round-trip. Select traceroute to target an IPv4 address or hostname. Select traceroute6 to target an IPv6 address. We do not support DNS resolution for hosts with IPv6 addresses. Hence, traceroute6 does not support traceroute to hostnames. • NSLookup-Use NSlookup to get detailed information about a name server on the network. You can query on several different types of information, including a server's IP address, alias IP address, start-of-authority record, mail exchange record, user information, well-known services information, and other types of information. • ARP-Use the arp command to map IP network addresses to the hardware addresses. The Address Resolution Protocol (ARP) allows you to resolve hardware addresses. To resolve the address of a server in your network, a system sends information about its unique identifier to a server process executed on a server in the intranet. The server process then returns the required address to the client process.

Settings	Guidelines
	AvgRTTs-Use AvgRTTs to display the average round-trip time (RTT) to the localhost.
	Portprobe-Display the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) port status (open or closed).
Target server	Specify the IP address or hostname for the target server.
Interface	Select the interface from which to send the command.
VLAN Port	Select a VLAN port, to test connectivity to a subscriber intranet.
Output	Displays command output.

Troubleshooting TCP and UDP Port Status

Problem	Description
Problem Description	The system makes several connections to back-end servers using various port numbers. If communication between the system and the back-end servers stops, it can be difficult to determine the source of the problem.
Solution	You can use the Portprobe command to display the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) port status (open or closed).

 Only the system internal ports, management port and internal VLAN ports support the Portprobe command.

A TCP port can be closed under two conditions:

- The system sends a connection request to the back-end server port and the back-end server closes the connection (sends an RST packet).
- The connection request times out because the back-end server is not found or the back-end server is too busy to respond to the connection request.

If either of these conditions occurs, the system sends a ping command to the back-end server. If the ping command is successful, the back-end server is considered reachable but the back-end server port is closed. If the ping command fails, the back-end server is considered unreachable.

For UDP ports, the system sends a UDP datagram with a ping to the back-end server port. If the back-end server responds with Internet Control Message Protocol (ICMP) port unreachable or ICMP unreachable, the back-end port is considered unreachable. If the back-end server responds with ICMP host unreachable then the back-end server is considered unreachable.

To troubleshoot the TCP or UDP port:

1. Select **Maintenance > Troubleshooting > Tools > Commands**.
2. Select the Portprobe command.
3. Select either **TCP** or **UDP**.
4. Enter the target server and port number. You can enter an IP address, hostname or FQDN for the target server.
5. Enter the probe count. This is the number of times the system attempts to communicate with the back-end server port. The default for TCP is one; the default for UDP is five.
6. Enter the probe timeout. This is the number of seconds the system waits for a response from the back-end server port.
7. Select either the internal port or the management port. If the management port is not configured, it is not displayed.
8. If using an internal port, select the internal VLAN port from the list.
9. Click **OK**.

The following figure shows an example of a successful and an unsuccessful port probe.

Troubleshooting > Tools > Commands

Commands

User Sessions | Monitoring | **Tools** | System Snapshot | Remote Debugging

TCP Dump | **Commands** | Kerberos | Licensing Protocol Trace

IPv6 is not supported

Command:

Protocol:

Target Server: Target port[1-65535]:

Probe Count: (default: tcp = 1, udp = 5, max = 100)

Probe Timeout: (default: 1 secs, max = 180 secs)

Interface: Internal Port Management Port

VLAN Port:

Output:

```
Resolving IP address for www.google.com
Resolved IP address: 172.217.18.68
Starting port probing

Tcp probe : 172.217.18.68:80 Open
Tcp probe : 172.217.18.68:80 Open
Tcp probe : 172.217.18.68:80 Open
Tcp probe : 172.217.18.68:80 Open
Tcp probe : 172.217.18.68:80 Open
Tcp probe : 172.217.18.68:80 Open

Operation complete
```

Troubleshooting > Tools > Commands

Commands

User Sessions | Monitoring | **Tools** | System Snapshot | Remote Debugging

TCP Dump | **Commands** | Kerberos | Licensing Protocol Trace

IPv6 is not supported

Command:

Protocol:

Target Server: Target port[1-65535]:

Probe Count: (default: tcp = 1, udp = 5, max = 100)

Probe Timeout: (default: 1 secs, max = 180 secs)

Interface: Internal Port Management Port

VLAN Port:

Output:

```
Resolving IP address for 10.209.118.10
Resolved IP address: 10.209.118.10
Starting port probing

UDP probe: 10.209.118.10:8888 Close ( Destination host is unreachable )
UDP probe: 10.209.118.10:8888 Close ( Destination host is unreachable )
UDP probe: 10.209.118.10:8888 Close ( Destination host is unreachable )
UDP probe: 10.209.118.10:8888 Close ( Destination host is unreachable )
UDP probe: 10.209.118.10:8888 Close ( Destination host is unreachable )

Operation complete
```

Testing Server Connectivity

To run NSLookup to test name server connectivity:

1. In the admin console, choose **Maintenance > Troubleshooting > Tools > Commands**.
2. From the Command list, select **NSLookup**.
3. Select the type of query to use from the Query Type drop down menu.

4. Enter the query, which is a hostname, an IP address, or other information, depending on your selection of query type.
5. Enter the VLAN port.
6. Click **OK** to run the command.

Troubleshooting > Tools > Commands

Commands

User Sessions | Monitoring | **Tools** | System Snapshot | Remote Debugging

TCP Dump | **Commands** | Kerberos | Licensing Protocol Trace

Command: NSLookup

Query Type: ANY - All available information

Query: Hostname, or IPv4/IPv6 address, or other information based on Query Type

Interface: Internal Port

VLAN Port: Internal Port (10.96.71.1)

OK **Clear**

Output: None

Kerberos Debugging

You can run the Kerberos debugging utility from the admin console. The utility checks the DNS infrastructure for validity of the Kerberos realms and defined credentials.

To use the Kerberos debugging utility:

1. Select **Maintenance > Troubleshooting > Tools > Kerberos** to display the configuration page.
2. Complete the configuration as described below.
3. Click **Run** to start the debugging process.
4. Click **Get to save the output to a file**, or click **Delete** to clear the output.

Troubleshooting > Tools > Kerberos

Kerberos

User Sessions | Monitoring | **Tools** | System Snapshot | Remote Debugging

TCP Dump | Commands | **Kerberos** | Licensing Protocol Trace

Probe Kerberos DNS Setup

Run

Output: None

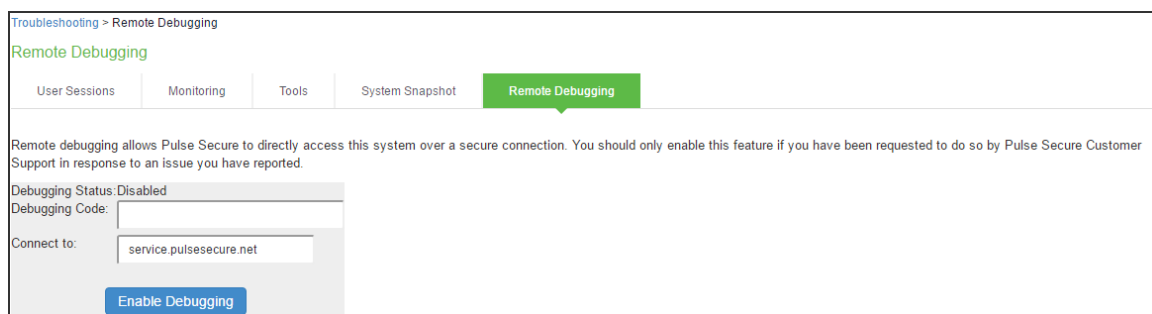
Settings	Guidelines
Probe Kerberos DNS Setup	Select this option to display the configuration elements for the Kerberos DNS test.
Kerberos Realm	Specify the realm name.
Site	Specify the fully qualified domain name.
Output	Displays results of the probe, for example: <pre>KDCs for realm matrix.net: top.matrix.net,top.matrix.net Operation complete</pre>

Remote Debugging

Remote debugging allows Ivanti Global Support Center to directly access this system over a secure connection. You should enable this feature only if you have been requested to do so by PSGSC in response to an issue that you have reported.

To enable remote debugging:

1. Select **Maintenance > Troubleshooting > Remote Debugging** to display the configuration page.
2. Complete the configuration and actions as described below.



Settings	Guidelines
Debugging Status	Displays whether remote debugging is enabled or disabled.
Debugging Code	Specify a code as instructed by PSGSC.

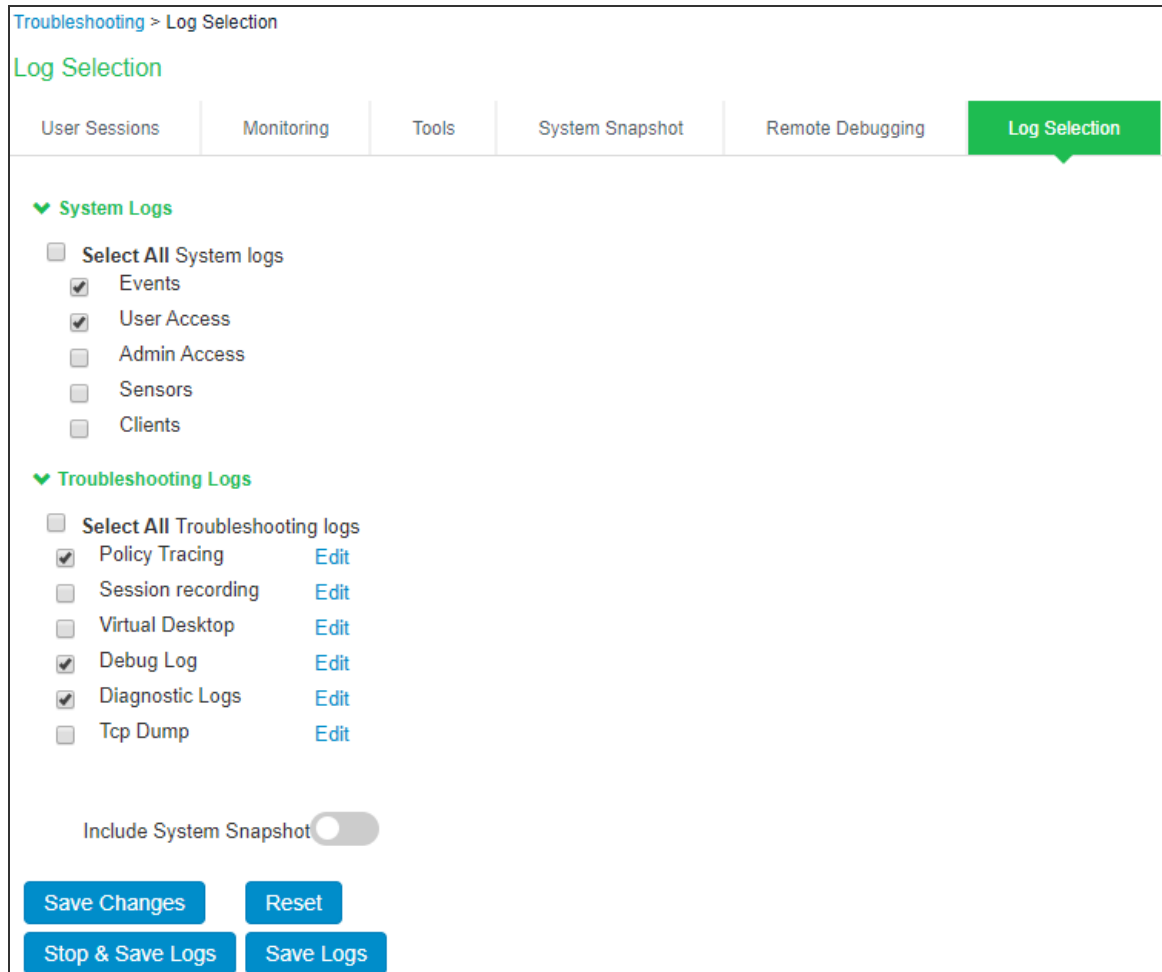
Settings	Guidelines
Connect to	Specify the fully qualified domain name as instructed by PSGSC.
Enable Debugging	Click this option to allow remote debugging.

Using Log Selection

The various system logs and troubleshooting logs that help in investigating user access issues and system issues can be configured and accessed from the Log Selection page.

To configure system logs and troubleshooting logs:

1. Select **Maintenance > Troubleshooting > Log Selection** to display the Log Selection page.



2. Complete the configuration and actions as described in the following table.


Settings	Guidelines
System Logs	
Select All System Logs	Select this check box to capture all system logs. To choose specific log, select individual system log from the list.
Troubleshooting Logs	
Select All Troubleshooting Logs	Select this check box to capture all troubleshooting logs. To choose specific log, select individual troubleshooting log from the list.

Settings	Guidelines
Edit log settings	To configure the settings of individual logs, click the corresponding Edit link. Complete the configuration and click Save Changes.
Stop and Save Logs	Stops the services used for the log collection and archives all the selected logs and then prompts to download the archive file.
Save Logs	Archives all the selected logs and prompts to download it as a bundle.


Troubleshooting the Common Issues with IPS

Table describes the common issues with IPS and provides the possible resolution.

Category	Description	Resolution/KB docs
Installation	Integrating Cisco IP phone 7941 or 7911G for 802.1x authentication with the IPS solution	For more information, see KB 13668 .
	Pulse Secure Desktop Client prompts for certificate validation even though the Trusted Root certificate is installed	For problem resolution, see KB 23479 .
	Communication Ports that are open by default on IPS device	For more information, see KB 24280 .
Layer 2 (802.1X, MAC Auth, SNMP, RADIUS)	802.1X- "TLS handshake failed" posted to the IPS user access log	For problem resolution, see KB 13716 .
	MAC Auth- Does IPS count MAC authentication against the concurrent user license?	For more information, see KB 24574 .
	SNMP monitoring of IPS devices	For more information, see KB 26207 .
	RADIUS dropped new Radius authentication request	For resolution, see KB 30167 .

Category	Description	Resolution/KB docs
Layer 3 (SRX, SOS, PAN, Fortinet)	Juniper SRX firewalls disconnect and reconnect at random times causing loss of access to protected resources	For resolution, see KB 40024 .
	Delay in removal of user session from Palo Alto Firewall after termination of session on IPS	For resolution, see KB 40165 .
Host Checker	Upgrading ESAP in an L2 authentication environment	For resolution, see KB 28732 .
	How to enforce domain membership with Host Checker Policy	For resolution, see KB 17389 .
IF-MAP	Information on IF-Map Server and IF-Map Client	For more information, see KB 22006 .
	Cannot find an option to enable IF-MAP server in admin GUI	For more information, see KB 23043 .
Cluster	Cluster VIP flapping between both of the nodes in Active/Passive cluster	For resolution, see KB 21584 .
	Cluster Licensing Best Practices	For more information, see KB 40093 .
	<p>Do the active nodes monitor the state of their own interface? Each node monitors both of it's interfaces by sending an ARP to the default gateway. This ARP message is sent every 5 seconds. The IPS waits up to 5 seconds for a response. If there is no response the IPS begins a wait period of 45 seconds. If there is still no response, the IPS marks the interface as down.</p> <hr/> <p> The ARP timeout value is configurable from the network settings page for each interface. Additionally, you can configure how many ARP ping timeouts are received before marking the interface as down. This applies to both interfaces and all nodes in the cluster. On the cluster properties page, there is an option to have each IPS disable their external interface in the event their internal interface goes down. This is a cluster-wide setting.</p> <hr/>	
	How big is the Synchronization Packet?	

Category	Description	Resolution/KB docs
	<p>This depends on how much data is synchronized. It is observed that approximately 1MB of data is transferred for 1000 users when a node is added to the cluster and synchronized. After the nodes are synchronized, data is sent only upon a status change. For example, user session status, user properties (bookmarks), or a change to the system configuration.</p>	
	<p>How does the IPS inform the local nodes if the passive becomes the Master? When one IPS fails, the other IPS detects the outage and assumes the VIP. It then issues a gratuitous ARP so that all local nodes (switches and routers included) will know the new MAC address for the VIP.</p>	
	<p>Explanation on LEADER cluster status and Sync Rank</p>	<p>For more information, see KB 13295.</p>
	<p>I have received my replacement IPS; how do I join it to my existing cluster?</p>	<p>For more information, see KB 13727.</p>
	<p>Procedure for replacing a device in an Active/Passive or Active/Active cluster</p>	<p>For more information, see KB 16146.</p>
	<p>Procedure to collect logs</p>	<p>For more information, see KB 21714.</p>
<p>AAA (AD, LADAP, RADIUS)</p>	<p>Users intermittently fail auth to Active Directory; NT_STATUS_IO_TIMEOUT seen in logs</p>	<p>For resolution, see KB 40179</p>
	<p>Does the IPS server support, multiple instances of Active Directory/Windows NT, for the same domain?</p>	<p>For resolution, see KB 21702.</p>
	<p>What permissions are needed on the service account used within ICS/IPS Active Directory standard mode authentication server and how to set it up using Delegate Control Wizard</p>	<p>For resolution, see KB 40401.</p>
	<p>Mapping based on Primary Group by using LDAP Authorization Server.</p>	<p>For more information, see KB 2527.</p>

Category	Description	Resolution/KB docs
Guest	<p>500 Internal Error, when attempting to sign into the GUAM portal</p> <hr/> <p> The customization for GUAM is no more supported from the IPS 5.2 release.</p> <hr/>	<p>For resolution, see KB 40296.</p>

Appendix REST API Support

Overview

The REST API provides a standardized method for Next-Gen firewalls and third-party systems to interact with IPS. **Representational state transfer (REST)** or RESTful Web services are one way of providing interoperability between computer systems on the Internet. REST-compliant Web services allow requesting systems to access and manipulate textual representations of Web resources using a uniform and predefined set of stateless operations. In a RESTful Web service, requests made to a resource's URI will elicit a response that may be in XML, HTML, JSON or some other defined format. IPS supports JSON format only.

REST methods determine the HTTP method for manipulating the resources defined in the service operation. The kind of operations available include those predefined by the HTTP verbs GET, POST, PUT, DELETE and so on. The response may confirm that some alteration has been made to the stored resource, and it may provide hypertext links to other related resources or collections of resources. By making use of a stateless protocol and standard operations, REST systems aim for fast performance, reliability, and the ability to grow, by re-using components that can be managed and updated without affecting the system as a whole, even while it is running.



REST API Support for IPS involves only Configuration APIs. IPS supports only the GET, POST, PUT and DELETE APIs.

The valid and supported values are described in table.

HTTP Verb	Definition
DELETE	Delete an existing resource.
GET	Retrieve a representation of a resource.
POST	Create a new resource
PUT	Create a new resource to a new URL, or modify an existing resource to an existing URL.

The error codes supported are described in the table.

HTTP Verb	Definition
200 OK	Requesting for resource information successful using GET Resource updation successful using PUT
201 Created	Resource creation successful using POST
204 No Content	Deletion of resource successful with no body. Even PUT, POST may return 204 if no errors or warnings seen
400 – Bad Request	Any Request (GET/PUT/POST/DELETE, and so on) is invalid. Example: Incorrect JSON format
401 – Unauthorized	Any REST Call with invalid credentials
403 – Forbidden	REST Call with valid credentials but no permission.
404 – Not found	Requested resource in URI does not exists
422 – Unprocessable Entity	Any validation/referential integrity errors that would result in failure of PUT/POST/DELETE request
500 Server Error	When IPS rest server is not responding

Authentication for REST APIs

Basic authentication using the HTTP authorization header is used to authenticate username/password on the Administrators authserver. It is expected that the user is already configured in the Administrators authserver. On a successful login, a random token (api_key) is generated and sent back as a JSON response. Further access to APIs can use this api_key in their Authorization header for access. The entire communication is over TLS. An example is explained below:

```

REQUEST
GET /api/v1/auth HTTP/1.1
Host: xx.xx.xx.xx
Authorization: Basic YWRtaW5kYjpkYW5hMTIz
Content-Type: application/json

RESPONSE
HTTP/1.1 200 OK
Cache-Control: no-store
Connection: Keep-Alive
Content-Type: application/json

```

```
Expires: -1
Keep-Alive: timeout=15
{ "api_key": "p5mM1c7RQu81R2NvssLCCZhP05kf0N2ONFeYeLXX6aU=" }
```

Authorization header for all future request should perform Basic Auth using above api_key value as username and password as empty.

```
REQUEST
GET /api/v1/configuration HTTP/1.1
Host: xx.xx.xx.xx
Authorization: Basic cDVtTWxjN1JRdTgxUjJ0dnNzTENDWmhQMDVrZjBOMk90RmVZZUxYWDZhVT06

RESPONSE
HTTP/1.1 200 OK
Content-Length ?283
Content-Type ?application/json
{ "
administrators":
{ "href": "/api/v1/configuration/administrators" }
, "
authentication":
{ "href": "/api/v1/configuration/authentication" }
, "
system":
{ "href": "/api/v1/configuration/system" }
, "
users":
{ "href": "/api/v1/configuration/users" }
}
```

Enabling REST API Configuration

The configuration of IPS can be accessed using REST APIs. The IPS configuration is represented in a JSON form when accessed using REST APIs. The structure of the JSON representation is very similar to the structure of IPS XML configuration.

A new admin UI option for users under "Administrators" authserver has been added. REST API authentication would be successful only for those users who have this option enabled.

To enable this checkbox:

1. Go to **Authentication > Auth. Servers > Administrators > Users > New/Update**.
2. Select the **Allow access to REST APIs** checkbox.
3. Click **Save Changes**.

Sample GET/POST/PUT/DELETE Request and Responses

Below is a sample of GET/POST/PUT/DELETE request and responses:

```
REQUEST
POST /api/v1/configuration/uac/infranet-enforcer/connections/infranet-enforcer/
HTTP/1.1
Host xx.xx.xx.xx
Authorization : Basic
VU9qSTlGTzNrYVYk5d0t2aXpBN1dPZ0FyZlN1S3FmTkNnQUh0R0ZuR0xSbz06
Content-Type: application/json
{
  "idp-for-local-sessions-only": "true",
  "junos": {
    "location-group": "- No 802.1X -",
    "password-encrypted":
      "3u+UR6n8AgABAAAofSnIBrU19vdwUs1G5LG4cg1QH6CbXDSmY4ZW0x85HY="
  },
  "name": "SRX",
  "serial-number": [
    "SJFIOQJI4KNM"
  ],
  "severity-filter": "medium",
  "use-idp": "false"
}
RESPONSE
HTTP/1.1 201 OK
Content-Length: 122
Content-Type: application/json
{
  "result": {
    "info": [
      {
        "message": "Operation succeed without warning or error!"
      }
    ]
  }
}
```

```
}
}
```

PUT API call: It will update the existing configuration. Configured Location Group as "Guest" and updated to "Default" Location group.

Before Updating the Location Group

```
REQUEST
GET api/v1/configuration/uac/network-access/radius-clients/radius-client/
Radius%20Client HTTP/1.1
Host xx.xx.xx.xx
Authorization : Basic
VU9qSTlGTzNrYVk5d0t2aXpBN1dPZ0FyZlN1S3FmTkNnQUh0R0ZuR0xSbz06
Content-Type: application/json
{
  "coa-support": "true",
  "description": "",
  "disconnect-support": "true",
  "dynamic-auth-port": "3799",
  "enable": "true",
  "gatewayid": "",
  "ip-address": "10.204.88.12",
  "ip-address-range": "1",
  "kek-encrypted": "",
  "key-wrap-format": "HEX",
  "key-wrap-support": "false",
  "location-group": "Guest",
  "mack-encrypted": "",
  "make-model": "Ruckus Wireless",
  "name": "Radius Client",
  "ruckus-certificate-verification": "false",
  "ruckus-password-encrypted": "",
  "shared-secret-encrypted":
  "3u+UR6n8AgABAAAofSnIBrU19vdwUs1G5LG4cg1QH6CbXDSmY4ZW0x85HY="
}
RESPONSE
HTTP/1.1 200 OK
Content-Length: 122
Content-Type: application/json
```

After Updating the Location Group

```
REQUEST
PUT api/v1/configuration/uac/network-access/radius-clients/radius-client/
Radius%20Client HTTP/1.1
Host xx.xx.xx.xx
Authorization : Basic
VU9qSTlGTzNrYVks5d0t2aXpBNldPZ0FyZlNlS3FmTkNnQUh0R0ZuR0xSbz06
Content-Type: application/json
{
  "coa-support": "true",
  "description": "",
  "disconnect-support": "true",
  "dynamic-auth-port": "3799",
  "enable": "true",
  "gatewayid": "",
  "ip-address": "xx.xxx.xx.xx",
  "ip-address-range": "1",
  "kek-encrypted": "",
  "key-wrap-format": "HEX",
  "key-wrap-support": "false",
  "location-group": "Default",
  "mack-encrypted": "",
  "make-model": "Ruckus Wireless",
  "name": "Radius Client",
  "ruckus-certificate-verification": "false",
  "ruckus-password-encrypted": "",
  "shared-secret-encrypted":
  "3u+UR6n8AgABAAAAofSnIBrU19vdwUslG5LG4cg1QH6CbXDSmY4ZW0x85HY="
} RESPONSE
HTTP/1.1 200 OK
Content-Length: 122
Content-Type: application/json
{
  "result": {
    "info": [
      {
        "message": "Operation succeed without warning or error!"
      }
    ]
  }
}
```


DELETE API Call: Deleting SNMP device from IPS

```
REQUEST
DELETE api/v1/configuration/uac/snmpEnforcement/clients/client/ruckus HTTP/1.1
Host 10.96.73.37
Authorization : Basic
VU9qSTlGTzNrYVks5d0t2aXpBN1dPZ0FyZlN1S3FmTkNnQUh0R0ZuR0xSbz06
Content-Type: application/json
{
  "default-vlan": "0",
  "description": "",
  "enable": "true",
  "ip-address": "10.204.88.12",
  "location-group": "none",
  "model": "Ruckus Wireless",
  "name": "ruckus",
  "read-auth-password-encrypted": "",
  "read-auth-protocol": "md5",
  "read-priv-password-encrypted": "",
  "read-priv-protocol": "",
  "read-security-level": "auth",
  "read-username": "public",
  "snmp-enforcement": "false",
  "snmp-version": "V2",
  "sys-contact": "https://support.ruckuswireless.com/contact_us",
  "sys-description": "Ruckus Wireless ZD1200",
  "sys-location": "350 West Java Dr. Sunnyvale, CA 94089 US",
  "sys-name": "ruckus",
  "trap-auth-password-encrypted": "",
  "trap-auth-protocol": "md5",
  "trap-priv-password-encrypted": "",
  "trap-priv-protocol": "",
  "trap-security-level": "auth",
  "trap-username": "public",
  "use-samecredential": "true",
  "write-auth-password-encrypted": "",
  "write-auth-protocol": "md5",
  "write-priv-password-encrypted": "",
  "write-priv-protocol": "",
  "write-security-level": "auth",
  "write-username": "public"
```

```
} RESPONSE  
HTTP/1.1 204 NO CONTENT  
Content-Length: 0  
Content-Type: application/json
```

Appendix Custom Expressions and System Variables Reference

Using Custom Expressions in Rule Configuration

This topic describes custom expressions. It is intended for advanced users.

Custom Expressions

Many system rules, such as role mapping rules or resource policy rules, support custom expressions. A custom expression is a combination of variables that the system evaluates as a Boolean object. The expression returns true, false, or error.


You can write custom expressions in the following formats. Note that elements of these formats are described in greater detail in the table that follows:

- *variable comparisonOperator variable*
- *variable comparisonOperator simpleValue*
- *variable comparisonOperator (simpleValue)*
- *variable comparisonOperator (OR Values)*
- *variable comparisonOperator (AND Values)*
- *variable comparisonOperator (time TO time)*
- *variable comparisonOperator (day TO day)*
- *isEmpty (variable)*
- *isUnknown (variable)*
- *(customExpr)*
- *NOT customExpr*
- *! customExpr*
- *customExpr OR customExpr*

- *customExpr || customExpr*
- *customExpr AND customExpr*
- *customExpr && customExpr*

Custom Expression Elements

Element	
<i>variable</i>	<p>Represents a system variable. A variable name is a dot-separated string, and each component can contain characters from the set [a-z A-Z 0-9_] but cannot start with a digit [0-9]. Variable names are case-insensitive. For system variables that you may use in role mapping rules and resource policies.</p> <p>When writing a custom expression in a log query field, you need to use system log variables. These variables are described in the Filter Variables Dictionary on the Filter page (System > Log/Monitoring > Events User Access Admin Access > Filters > Select Filter tab).</p> <p>Quoting syntax for variables:</p> <p>The system supports a quoting syntax for custom expression variables that allows you to use any character except '.' (period) in a user attribute name. To escape characters in an attribute name, quote some or all of the variable name using {} (curly-braces). For example, these expressions are equivalent: <code>userAttr.{Login-Name} = 'xyz'</code> <code>userAttr.Login{-}Name = 'xyz'</code> <code>{userAttr.Login-Name} = 'xyz'</code> <code>userA{ttr.L}{ogin{-}Name = 'xyz'</code></p> <p>Escape characters supported within quotes:</p> <ul style="list-style-type: none"> • <code>\\</code> — Escape a backslash (\) • <code>\{</code> — Escape a left curly brace ({) • <code>\}</code> — Escape a right curly brace (}) • <code>\hh</code> — Escape a hexadecimal value where hh is two characters from [0-9A-Fa-f] <p>Examples:</p> <pre>userAttr.{Tree Frog} = 'kermit' userAttr.{Tree\20Frog} = 'kermit'</pre>

Element	
	<hr/> <ul style="list-style-type: none"> - There is no limit to the number of quotes you can use in a variable name.  - You can use the quoting syntax with any variable, not just userAttr.* variables - You need to use curly-brace quotes only when writing custom expressions. <hr/>
<i>comparisonOperator</i>	<p>One of the following:</p> <ul style="list-style-type: none"> • = — Equal to. Use with strings, numbers, and DNs. • != — Not equal to. Use with strings, numbers, and DNs. • < — Less than. Use with numbers. • <= — Less than or equal to. Use with numbers. • > — Greater than. Use with numbers. • >= — Greater than or equal to. Use with numbers.
<i>simpleValue</i>	<p>One of the following:</p> <ul style="list-style-type: none"> • <i>string</i> — quoted string that may contain wildcards. • <i>IP Address</i> — a.b.c.d • <i>subnet</i> — a.b.c.d/subnetBitCount or a.b.c.d/netmask • <i>number</i> — Positive or negative integer • <i>day</i> — SUN MON TUE WED THU FRI SAT <p>Notes about strings: A string may contain all characters except <nl> (newline) and <cr> (carriage return). Strings can be any length. String comparisons are case-insensitive. Strings can be quoted with single- or double-quotes. A quoted string may contain wildcards, including star(*), question mark (?), and square brackets ([]).</p>

Element	
	<p>variable comparisonOperator variable comparisons are evaluated without wildcard matching.</p> <p>Use a backslash to escape these characters:</p> <ul style="list-style-type: none"> • single-quote (') — \' • double-quote (") — \" • backslash (\) — \\ • hexadecimal — \hh [0-9a-fA-F] <p>Note about day: Day and time comparisons are evaluated in the system's time zone. Day range (day TO day) calculations start with the first day and step forward until the second day is reached. In time range (time TO time) calculations, the first value must be earlier than the second value. Only time variables can be compared to day and time values. The time variables are: time.* and log inTime.*.</p>
<i>time</i>	<p>Time of day in one of the following formats:</p> <p><i>HH:MM</i> — 24-hour <i>HH:MMam</i> — 12-hour <i>HH:MMpm</i> — 12-hour <i>H:MM</i> — 24-hour <i>H:MMam</i> — 12-hour <i>H:MMpm</i> — 12-hour</p> <p>Day and time comparisons are evaluated in the system's time zone. Day range (day TO day) calculations start with the first day and step forward until the second day is reached. In time range (time TO time) calculations, the first value must be earlier than the second value. Only time variables can be compared to day and time values. The time variables are: time.* and log inTime.*.</p>
<i>OR Value</i>	<p>String containing one or more OR comparisons:</p> <p>Examples: <i>variable comparisonOperator (number OR number ...)</i> <i>variable comparisonOperator (string OR string ...)</i></p>
<i>AND Value</i>	<p>String containing one or more AND comparisons.</p>

Element	
	Examples: <i>variable comparisonOperator (number AND number ...)</i> <i>variable comparisonOperator (string AND string ...)</i>
<i>isEmpty</i>	Function that takes a single variable name (variable) argument and returns a boolean value. isEmpty() is true if the variable is unknown or has a zero-length value, zero-length strings, and empty lists. Example: isEmpty(userAttr.terminationDate)
<i>isUnknown</i>	Function that takes a single variable name (variable) argument and returns a boolean value. isUnknown() is true if the variable is not defined. User attributes (userAttr.* variables) are unknown if the attribute is not defined in LDAP or if the attribute lookup failed (such as if the LDAP server is down). Example: isUnknown(userAttr.bonusProgram)
<i>NOT, !</i>	Logical negation comparisonOperator. The negated expression evaluates to true if the customExpr is false and evaluates to false if the customExpr is true. The operators NOT, AND, and OR are evaluated from highest to lowest precedence in this order: NOT (from right), AND (from left), OR (from left).
<i>OR, </i>	Logical operator OR , which are equivalent. The operators NOT, AND, and OR are evaluated from highest to lowest precedence in this order: NOT (from right), AND (from left), OR (from left).
<i>AND, &&</i>	Logical AND or &&, which are equivalent. The operators NOT, AND, and OR are evaluated from highest to lowest precedence in this order: NOT (from right), AND (from left), OR (from left).
<i>customExpr</i>	Expression written in the Custom Expression Syntax (see above).

Wildcard Matching

In a quoted string, supported wildcards include:

- star (*)—A star matches any sequence of zero or more characters.
- question mark (?)—A question mark matches any single character.

- square brackets ([])—Square brackets match one character from a range of possible characters specified between the brackets. Two characters separated by a dash (-) match the two characters in the specified range and the lexically intervening characters. For example, 'dept[0-9]' matches strings "dept0", "dept1", and up to "dept9".

To escape wildcard characters, place them inside square brackets. For example, the expression 'userAttr.x = " value [*]" ' evaluates to true if attribute x is exactly "value*".

Using Multivalued Attributes

Multivalued attributes—attributes that contain two or more values—provide you with a convenient method for defining resources that expand into multiple individual bookmarks on the users' bookmarks page.

For example, assume that the user's LDAP directory contains the multivalued attribute HomeShares: \\Srv1\Sales;\\Srv2\Marketing. When you configure the Windows File share resource definition using the HomeShares multivalued attribute, \\<userAttr.HomeShares>, the user sees two bookmarks:

- \\Srv1\Sales
- \\Srv2\Marketing

Now let's assume the user's LDAP directory contains a second multivalued attribute defined as HomeFolders: Folder1;Folder2;Folder3. When you configure the Windows File share resource using both of the multivalued attributes, \\<userAttr.HomeShares>\<userAttr.HomeFolders>, the user sees the following six bookmarks:

- \\Srv1\Sales\Folder1
- \\Srv1\Sales\Folder2
- \\Srv1\Sales\Folder3
- \\Srv2\Marketing\Folder1
- \\Srv2\Marketing\Folder2
- \\Srv2\Marketing\Folder3

The only exception to this functionality is when the variable includes an explicit separator string. In this case, only one bookmark containing multiple resources displays on the users' bookmark page.

You specify the separator string in the variable definition using the syntax `sep='string'` where string equals the separator you want to use. For example, to specify a semi-colon as the separator, use the syntax `<variable.Attr sep='; '>`.

Use the following syntax for multivalued attributes handling. Note that `<variable>` refers to a session variable such as `<userAttr.name>` or `<CertAttr.name>`:

`<variable[Index]>`—You specify indexes in a variety of ways. If, for example, the total number of values for a given index is 5, and you want to specify the entire range of values you use `<variable[ALL]>`. If you want to specify only the fourth value, you use `<variable[4]>`.

- `<variable>` is the same as `<variable[ALL]>`.
- `<variable>` is the same as `<variable[ALL]>`.
- `<variable sep='str'>` and `<variable[All] sep='str'>` — These variable definitions always refer to a single string value with all the tokens expanded out with separator strings between the values.



Variable names cannot contain spaces.

Specifying Multivalued Attributes in a Bookmark Name

Another common case of using multivalued attributes occurs when you include a variable in a bookmark name and in a URL or file server/share field.

For example, again assume that the user's LDAP directory contains the multivalued attribute HomeShares: `\\Srv1\Sales;\\Srv2\Marketing`. When you configure the Windows File share resource definition using the HomeShares multivalued attribute, `\\<userAttr.HomeShares>`, and you use the same attribute in the bookmark name field, `<userAttr.HomeShares>`, the system creates two bookmarks:

- `Srv1\Sales` bookmark pointing to `\\Srv1\Sales`
- `Srv2\Marketing` bookmark pointing to `\\Srv2\Marketing`

This does not create a situation in which you end up with the following set of conditions:

- `Srv1\Sales` bookmark pointing to `\\Srv1\Sales`
- `Srv1\Marketing` bookmark pointing to `\\Srv1\Marketing` (error)

- Srv2\Sales bookmark pointing to \\Srv1\Sales (error)
- Srv2\Marketing bookmark pointing to \\Srv2\Marketing

Distinguished Name Variables

You can compare a distinguished name (DN) to another DN or to a string, but the system ignores wildcards, white space, and case. Note, however, that the system takes the order of DN keys into consideration.

When the system compares an expression to a DN to a string, it converts the string to a distinguished name before evaluating the expression. If the system cannot convert the string due to bad syntax, the comparison fails. The DN variables are:

- userDN
- certDN
- certIssuerDN

The system also supports DN suffix comparisons using the **matchDNSuffix** function. For example:

```
matchDNSuffix( certDn, "dc=danastreet,dc=net")
```

Within the parenthesis, the first parameter is the "full" DN and the second is the suffix DN. You can use a or string for each parameter. Note that this first parameter should have more keys than the second (suffix parameter). Otherwise, if they are equal, it is the same as <firstparam> = <secondparam>. If the second parameter has more keys, matchDNsuffix returns false.

System Variables

The below table lists and defines system variables, gives an example for each system variable, and provides a guide as to where you may use system variables.

Variable	Description	Usage	Examples
authMethod	Type of authentication method used to authenticates a user.	role mapping rules, resource policy rules	authMethod = 'ACE Server'

Variable	Description	Usage	Examples
cacheCleanerStatus	The status of Cache Cleaner. Possible values: 1 - if it is running 0 - if otherwise		cacheCleanerStatus = 1 cacheCleanerStatus = 0


Variable	Description	Usage	Examples
certAttr.<cert-attr>	<p>Attributes from a client-side certificate. Examples of certAttr attributes include:</p> <ul style="list-style-type: none"> • C - country • CN - common name • description - description • e-mailAddress - e-mail address • GN - given name • initials - initials • L - locality name • O - organization • OU - organizational unit • SN - surname • serialNumber- serial number • ST - state or province • title - title • UI - unique identifier <p>Use this variable to check that the user's client has a client-side certificate with the value(s) specified.</p>	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields • LDAP configuration 	<p>certAttr.OU = 'Retail Products Group'</p>

Variable	Description	Usage	Examples
certAttr.altName.<Alt-attr>	<p>Subject alternative name value from a client-side certificate where <Alt-attr> may be:</p> <ul style="list-style-type: none"> • Email • EmailId • EmailDomain • DNS • registeredId • ipAddress • UPN • UPNid • UPNDomain • fascn • fascnAC • fascnSC • fascnCN • fascnCS • fascnCI • fascnPI • fascnOC • fascnOI • fascnPOA • fascnLRC 	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields • LDAP configuration 	<ul style="list-style-type: none"> • certAttr.altName.ipAddress = 10.10.83.2 • certAttr.altName.email = "joe@company.com"


Variable	Description	Usage	Examples
certAttr.serialNumber	Client certificate serial number. Note that all characters other than [0-9 a-f A-F] are stripped out of a string before comparison with certAttr.SN. Wildcards are not supported.	<ul style="list-style-type: none"> role mapping rules resource policy rules SSO parameter fields LDAP configuration 	<ul style="list-style-type: none"> certAttr.SerialNumber = userAttr.certSerial certAttr.SerialNumber = "6f:05:45:ab"
certDN	Client certificate subject DN. Wildcards are not permitted.	role mapping rules, resource policy rules	<ul style="list-style-type: none"> ·certDN = userDN (match the certificate subject DN with the LDAP user DN) certDN = userAttr.x509SubjectName certDN = ('cn=John Harding,ou=eng,c=Company' or 'cn=Julia Yount,ou=eng,c=Company')
certDN.<subject-attr>	Any variable from the client certificate subject DN, where subject-attr is the name of the RDN key.	<ul style="list-style-type: none"> role mapping rules 	<ul style="list-style-type: none"> certDN.OU = 'company'


Variable	Description	Usage	Examples
	Use to test the various subject DN attributes in a standard x.509 certificate.	<ul style="list-style-type: none"> • resource policy rules • SSO parameter fields • LDAP configuration 	<ul style="list-style-type: none"> • certDN.E = 'joe@company.com' • certDN.ST = 'CA'
certDNText	Client certificate user DN stored as a string. Only string comparisons to this value are allowed.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	<ul style="list-style-type: none"> • certDNText = 'cn=John Harding,ou=eng,c=Company'
certIssuerDN	Client certificate-issuer subject DN. This variable works like a standard DN attribute such as CertDN. Wildcards are not permitted.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	<ul style="list-style-type: none"> • certIssuerDN = 'cn=John Harding,ou=eng,c=Company' • certIssuerDN = userAttr.x509Issuer • certIssuerDN = ('ou=eng,c=Company' or 'ou=operations,c=Company')

Variable	Description	Usage	Examples
certIssuerDN.<issuer-attr>	Any variable from the client certificate-issuer subject DN, where issuer-attr is the name of the RDN key.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	<ul style="list-style-type: none"> • certIssuerDN.OU = 'company' • certIssuerDN.ST = 'CA'
certIssuerDNText	Client certificate-issuer subject DN stored as a string. Only string comparisons to this value are allowed.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	<ul style="list-style-type: none"> • certIssuerDNText = 'cn=John Harding,ou=eng,c=Company'
defaultNTDomain	Contains the Domain value set in the authentication server configuration when you use AD/NT authentication.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	defaultNTDomain="CORP"

Variable	Description	Usage	Examples
group.<group-name>	User's group membership as provided by the realm authentication or directory server.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules 	<ul style="list-style-type: none"> • group.preferredPartner • group.goldPartner or group.silverPartner • group.employees and time.month = 9 • Combination examples: • Allow all partners with active status from Monday to Friday but preferred partners Monday through Saturday: • ((group.partners and time = (Monday to Friday)) or • (group.preferredPartners and time = (Monday to Saturday)) and userAttr.partnerStatus = 'active' <hr/> <p> Spaces are not supported, such as, group.sales managers</p> <hr/>

Variable	Description	Usage	Examples
		<ul style="list-style-type: none"> Only those groups evaluated for role mapping rules are available in the detailed rules (conditions) in the resource policies. We recommend that you use the groups variable instead of <code>group.<group-name></code>, which is supported only for backwards compatibility. 	

Variable	Description	Usage	Examples
Groups	<p>List of groups as provided by the realm authentication or directory server.</p> <hr/> <p> You can enter any characters in the groupname, although wildcard characters are not supported.</p> <hr/>	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	groups=('sales managers')
hostCheckerPolicy	Host Checker polices that the client has met.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	hostCheckerPolicy = ('Norton' and 'Sygate') and cacheCleanerStatus = 1hostCheckerPolicy = ('Norton' and 'Sygate')
log inHost	Hostname or IP address that the browser uses to contact the Ivanti service.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	log inHost = 10.10.10.10

Variable	Description	Usage	Examples
		<ul style="list-style-type: none"> LDAP configuration 	
log inTime	<p>The time of day at which the user submits his credentials. The time is based on system time.</p> <hr/> <p> When using this variable in an SSO parameter field, the variable returns the UNIX string time.</p> <hr/>	<ul style="list-style-type: none"> role mapping rules resource policy rules SSO parameter fields 	<ul style="list-style-type: none"> log inTime = (8:00am) log inTime= (Mon to Fri)
log inTime.day	<p>The day of month on which the user submits his credentials, where day is 1-31. The time is based on the system time. You cannot use the TO operator with this variable.</p>	<p>role mapping rules resource policy rules</p>	log inTime.day = 3
log inTime.dayOfWeek	<p>The day of the week on which the user submits his credentials, where dayOfWeek is in the range [0-6] where 0 = Sunday.</p>	<ul style="list-style-type: none"> role mapping rules resource policy rules 	<ul style="list-style-type: none"> log inTime.dayOfWeek = (0 OR 6) log inTime.dayOfWeek = (mon TO fri) log inTime.dayOfWeek = (1) log inTime.dayOfWeek = 5

Variable	Description	Usage	Examples
	<p>The system does not support the TO operator with time.dayOfWeek expressions if you use numbers instead of strings. In other words, " log inTime.dayOfWeek = (2 TO 6)" does not work, but " log inTime.dayOfWeek = (mon to fri)" does work.</p>		
log inTime.dayOfYear	<p>The numeric day of the year on which the user submits his credentials, where dayOfYear can be set to [0-365]. You cannot use the TO operator with this variable.</p>	<ul style="list-style-type: none"> • role mapping rules • resource policy rules 	<ul style="list-style-type: none"> • log inTime.dayOfYear = 100
log inTime.month	<p>The month in which the user submits his credentials, where month can be set to [1-12] where 1 = January. You cannot use the TO operator with this variable.</p>	<ul style="list-style-type: none"> • role mapping rules • resource policy rules 	log inTime.month >= 4 AND log inTime.month <=9
log inTime.year	<p>The year in which the user submits his credentials, where year can be set to [1900-2999]. You cannot use the TO operator with this variable.</p>	<ul style="list-style-type: none"> • role mapping rules • resource policy rules 	log inTime.year = 2005

Variable	Description	Usage	Examples
log inURL	URL of the page that the user accessed to sign in. The system gets this value from the Administrator URLs User URLs column on the Authentication > Signing In > Sign-in Policies page of the admin console.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields • LDAP configuration 	log inURL = */admin
networklf	The network interface on which the user request is received. Possible values: internal, external	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	sourceIp = 192.168.1.0/24 and networkIf = internal
Ntdomain	The NetBIOS NT domain used in NT4 and Active Directory authentication.	<ul style="list-style-type: none"> • role mapping rules • SSO parameter fields 	ntdomain = jnpr

Variable	Description	Usage	Examples
Ntuser	The NT username used in Active Directory authentication	<ul style="list-style-type: none"> role mapping rules SSO parameter fields 	ntuser = jdoe password password[1]
password[2]	The password entered by the user for the primary authentication server (password and password[1]) or the secondary authentication server (password[2]).	<ul style="list-style-type: none"> role mapping rules resource policy rules SSO parameter fields 	password = A1defo2z
Realm	The name of the authentication realm to which the user is signed in.	<ul style="list-style-type: none"> role mapping rules resource policy rules SSO parameter fields 	Realm = ('GoldPartners' or 'SilverPartners') <hr/> AND condition will always fail as a user is only allowed to sign in to a single realm in a session. <hr/>
Role	List of all the user roles for the session. Role = ('Sales' AND 'Support')	<ul style="list-style-type: none"> resource policy rules 	<ul style="list-style-type: none"> Role = ('sales' or 'engineering') "Role = ('Sales' AND 'Support')

Variable	Description	Usage	Examples
	<p>In SSO, if you want to send all the roles to back-end applications, use <role sep = ";"> - where sep is the separator string for multiple values. The system supports all separators except " and >.</p>	<ul style="list-style-type: none"> SSO parameter fields 	
<p>radius.requestAttributes.<reqAttr></p>	<p>The list of default value are as follows:</p> <ul style="list-style-type: none"> radius.requestAttributes.Calling-Station-Id = <ANY> radius.requestAttributes.NAS-IP-Address = <ANY> radius.requestAttributes.NAS-Identifier = <ANY> radius.requestAttributes.NAS-Port-Type = <ANY> radius.requestAttributes.Called-Station-Id = <ANY> radius.requestAttributes.Aruba-Essid-Name = <ANY> radius.requestAttributes.User-Name = <ANY> 	<p>role mapping rules</p>	<p>radius.requestAttributes.Calling-Station-Id = "00:aa:3f:*</p>

Variable	Description	Usage	Examples
locationGroup	Allows the user to filter the roles based on the location group.	role mapping rules	locationGroup = "bangalore"
eapProtocol.<protocolLayer>	Allows the user to filter the roles based on EAP protocol. <protocolLayer> indicates whether the variable matches the inner protocol or outer protocol. <ul style="list-style-type: none"> The values for the outerProtocol variable are EAP-PEAP and EAP-TTLS. The values for the innerProtocol are PAP, CHAP, MS-CHAP, MS-CHAP-V2, EAP-MD5, EAP-TLS, EAP-MSCHAP-V2, EAP-GTC, and EAP-JUAC. 	<ul style="list-style-type: none"> role mapping rules 	eap-protocol.outerProtocol != "EAP-PEAP"
sourceIP	The IP address of the machine on which the user authenticates. You can specify the netmask using the bit number or in the netmask format: '255.255.0.0'. Note that you can evaluate the sourceIP expression against a string variable such as an LDAP attribute.	<ul style="list-style-type: none"> role mapping rules resource policy rules SSO parameter fields 	<ul style="list-style-type: none"> sourceIP = 192.168.10.20 sourceIP = 192.168.1.0/24 and networkIf internal userAttr.dept = ('eng' or 'it') and sourceIP = 10.11.0.0/16

Variable	Description	Usage	Examples
			<ul style="list-style-type: none"> sourceIP = 192.168.10.0/24 (Class C) <p>is the same as:</p> <ul style="list-style-type: none"> sourceIP = 192.168.10.0/255.255.255.0 sourceIP=userAttr.sourceip
Time	The time of day at which the role mapping rule or resource policy rule is evaluated. The time of the day can be in 12-hour or 24-hour format.	role mapping rules resource policy rules	<ul style="list-style-type: none"> time = (09:00 to 17:00) time = (Mon to Fri) time = (9:00am to 5:00pm) <p>Combination examples: Allow executive managers and their assistants access from Monday to Friday: userAttr.employeeType = ('*manager*' or '*assistant*') and group.executiveStaff and time = (Mon to Fri)</p>
time.dayOfWeek	The day of the week on which the role mapping rule or resource policy rule is evaluated, where dayOfWeek is in the range [0-6] where 0 = Sunday.	<ul style="list-style-type: none"> role mapping rules 	<ul style="list-style-type: none"> log inTime.dayOfWeek = (0 OR 6) log inTime.dayOfWeek = (1 to 5) log inTime.dayOfWeek = 5

Variable	Description	Usage	Examples
		<ul style="list-style-type: none"> resource policy rules 	
time.dayOfYear	The day of the year on which the role mapping rule or resource policy rule is evaluated. Possible values include: 1-365.	<ul style="list-style-type: none"> role mapping rules resource policy rules 	time.dayOfYear = 100
time.month	The month in which the role mapping rule or resource policy rule is evaluated. Possible values include: 1-12	<ul style="list-style-type: none"> role mapping rules resource policy rules 	time.month >= 9 and time.month <= 12 and time.year = 2004 group.employees and time.month = 9
time.year	The year in which the role mapping rule or resource policy rule is evaluated, where year can be set to [1900-2999].	<ul style="list-style-type: none"> role mapping rules resource policy rules 	time.year = 2005

Variable	Description	Usage	Examples
<p>user user@primary_auth_server_name user@secondary_auth_server_name</p>	<p>Ivanti username for the user's primary authentication server (user@primary_auth_server_name) or secondary authentication server (user@secondary_auth_server_name). Use when authenticating against an Active Directory server, domain and username. primary_auth_server_name is the name of the primary auth server. If there are spaces or special characters in the name, it can be enclosed in curly brackets. For example user@{My Primary Auth Server} secondary_auth_server_name is the name of the secondary auth server. If there are spaces or special characters in the name, it can be enclosed in curly brackets. For example user@{My Secondary Auth Server}</p> <hr/> <p>When including a domain as part of a username, you must include two slashes between the domain and user. For example: user='yourcompany.net\joeuser'.</p>	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	<ul style="list-style-type: none"> • user = 'steve' • user = 'domain\steve'

Variable	Description	Usage	Examples
<p>username username@primary_auth_server_name username@secondary_auth_server_name</p>	<p>Pulse Secure system username for the user's primary authentication server (username and username@primary_auth_server_name) or secondary authentication server (username@secondary_auth_server_name). If the user is signing in to a certificate authentication server, then the user's Ivanti system username is the same as CertDN.cn. primary_auth_server_name is the name of the primary auth server. If there are spaces or special characters in the name, it can be enclosed in curly brackets. For example user@{My Primary Auth Server} secondary_auth_server_name is the name of the secondary auth server. If there are spaces or special characters in the name, it can be enclosed in curly brackets. For example user@{My Secondary Auth Server}</p>	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	<ul style="list-style-type: none"> • username = 'steve' and time = mon • username = 'steve' • username = 'steve*' • username = ('steve' or '*jankowski')
<p>userAgent</p>	<p>The browser's user agent string.</p>	<ul style="list-style-type: none"> • role mapping rules 	<p>The browser's user agent string.</p>

Variable	Description	Usage	Examples
		<ul style="list-style-type: none"> • resource policy rules • SSO parameter fields 	

Variable	Description	Usage	Examples
userAttr.<auth-attr>	User attributes retrieved from an LDAP, RADIUS, or SiteMinder authentication or directory server.	role mapping rules resource policy rules SSO parameter fields	<p>userAttr.building = ('HQ*' or 'MtView[1-3]')</p> <p>userAttr.dept = ('sales' and 'eng')</p> <p>userAttr.dept = ('eng' or 'it' or 'custsupport')</p> <p>userAttr.division = 'sales'</p> <p>userAttr.employeeType != 'contractor'</p> <p>userAttr.salaryGrade > 10</p> <p>userAttr.salesConfirmed >= userAttr.salesQuota</p> <p>Negative examples:</p> <p>userAttr.company != "Acme Inc" or not group.contractors</p> <p>not (user = 'guest' or group.demo)</p> <p>Combination examples:</p> <p>Allow executive managers and their assistants access from Monday to Friday:</p> <p>userAttr.employeeType = ('*manager*' or '*assistant*')</p> <p>and group.executiveStaff</p> <p>and time = (Mon to Fri)</p> <p>Allow all partners with active status from Monday to Friday but preferred partners Monday through Saturday:</p> <p>((group.partners and time = (Mon to Fri)) or</p>

Variable	Description	Usage	Examples
			(group.preferredPartners and time = (Mon to Sat))) and userAttr.partnerStatus = 'active'
userDN	The user DN from an LDAP server. If the user is authenticated by the LDAP server, then this DN is from the authentication server; otherwise, the DN comes from the realm's Directory/Attribute server. Wildcards are not permitted.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules 	userDN = 'cn=John Harding,ou=eng,c=Company' userDN = certDN
userDN.<user-attr>	Any variable from the user DN, where user-attr is the name of the RDN key.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules • SSO parameter fields 	Any variable from the user DN, where user-attr is the name of the RDN key.
userDNText	User DN stored as a string. Only string comparisons to this value are allowed.	<ul style="list-style-type: none"> • role mapping rules • resource policy rules 	userDNText = 'cn=John Harding,ou=eng,c=Company'

Variable	Description	Usage	Examples
		<ul style="list-style-type: none"> SSO parameter fields 	

Custom Variables and Macros

Custom variables, like system variables, are name-value pair tags that you can use when defining role mapping rules, resource policy rules and SSO parameter fields.

Custom variables are created in the Server Catalog (for example, Authentication > Auth Server > *Name* > Settings) by using a predefined macro on a system variable. Available macros are:

- REGMATCH** – Matches a regular expression pattern against a string text.
- APPEND** – Appends a text string to another text string.
- DAYSDIFF** – Calculates the difference between two dates.



These macros are located under Variable Operators in the Variables tab of the Server Catalog window.

A custom variable name is a dot-separated string. Each component can contain characters from the set [a-z A-Z 0-9 _] but cannot start with a digit [0-9]. Custom variable names are case-insensitive.

Custom variables are referenced as **customVar.<variableName>**. For example, if you create a custom variable with the name **check-prefix**, you reference this custom variable as **customVar.check-prefix**.

append

Syntax	APPEND (attr, TextString) APPEND (attr, attr2)
Description	Append a text string to an attribute or append an attribute to another attribute and store the resulting string in the custom variable.
Options	attr —System variable of type string. TextString —Quoted ASCII string. attr2 —System variable of type string.

Output Fields	Returns a String value. If no match is found, returns an empty string If the system variable is multivalued, the custom variable is also multivalued and uses the same order as the system variable.
----------------------	---

Sample Output

APPEND (userName, "@sample.net")

In this example, the string "@sample.net" is appended to the userName value.

daysdiff

Syntax	DAYSDIFF (attr, timeformat)
Description	Calculates the number of days between the attribute and the current time.
Options	attr —System variable of type string.
	timeformat —Output time format. Valid values are: UTC, TIMET, MMDDYYYY
Output Fields	Returns an Integer value.

Sample Output

DAYSDIFF (certAttr.validUpto, UTC)

In this example, calculate the difference in days between the current time and the value of certAttr.validUpto and express the time in UTC (Coordinated Universal Time).

regmatch

Syntax	REGMATCH (attr, regex, groupingNumber)
Description	Match the regular expression pattern against an attribute and store the result in the custom variable. attr —System variable of type string. regex —Quoted string containing the regular expression to be applied to the attr option. groupingNumber —The group value to assign to the custom variable.

Additional Information	The regular expression supports the Perl Compatible Regular Expressions (PCRE) syntax. A grouping (capture buffer) in the regex pattern can also be used to define a custom variable.
Output Fields	Returns a String value. If no match is found, returns an empty string. If the system variable is multivalued, the custom variable is also multivalued and uses the same order as the system variable.

Sample Output

```
REGMATCH (mailId, "^(.*)@sample.net$", 1)
```

In this example, a mailId of myName@sample.net creates a custom variable with value "myName".

Specifying Fetch Attributes in a Realm

To facilitate the support for various parameterized settings in user roles and resource policies, you have the ability to specify additional fetch attributes. The system stores the fetch attributes when users log in so that you can use them in parameterized role or resource policy definitions.

The system pulls all the attributes that are currently stored in the Sever Catalog for the user's authentication or authorization LDAP server. So, make sure to add the LDAP user attributes that are used in role or resource policy definitions in the LDAP Server Catalog first.

When a user logs in, the system retrieves user attributes that are referenced in the role mapping rules plus all of the additional attributes referenced in the Server Catalog and stores all these values. Note that this should not incur a significant performance overhead because all the user attributes are retrieved in one single LDAP query.



When you substitute variables, such as in IP/Netmasks or hostnames, the values in the session are appropriately converted into the data type that is required by the particular application definition.

Specifying the homeDirectory Attribute for LDAP

You can create a bookmark that automatically maps to a user's LDAP home directory. You can accomplish this using the LDAP attribute homeDirectory. You need to configure a realm that specifies the LDAP server instance as its auth server, and you need to configure role-mapping rules and a bookmark that points to the LDAP homeDirectory attribute.