IBM Proventia® Management SiteProtector™ System

Policies and Responses Configuration Guide

Version 2.0, Service Pack 7.0

IBM Internet Security Systems

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.

September 17, 2009

Contents

Preface

Overview . . . 5
How to Use SiteProtector Documentation . . . 6
Getting technical support . . . 7
. . . 8

Part I: Managing Policies in the Repository

Chapter 1: Introduction to Policy Management

Overview . . . 11
The Policy View . . . 12
Upgrading from SP 6.1 to SP 7.0 . . . 13
Policy Permissions . . . 15

Chapter 2: The Policy Repository

Overview . . . 17
What is the Policy Repository? . . . 18
Working with Multiple Repositories . . . 19
Shared Objects . . . 20
Managing Policies in the Repository . . . 21
Importing and Exporting Policies . . . 23
Policy Deployment . . . 24
Migrating agent policy versions . . . 26

Chapter 3: Working with Policies at the Group Level

Overview . . . 27
Viewing Policy Deployments . . . 28
Policy Inheritance . . . 29
Policy Subscription Groups . . . 30

Chapter 4: Locally Configured Agents

Overview . . . 31
Locally Configured Agents . . . 32
Migrating Locally Configured Agents into SiteProtector . . . 33

Part II: Configuring Central Responses

Chapter 5: Working with Central Responses

Overview . . . 37
What are Central Responses? . . . 38
Creating Central Responses . . . 39

Chapter 6: Defining Response Objects

Overview . . . 41
What are Response Objects? . . . 42

Configuring E-mail Response Objects . . . 43
Configuring SNMP Response Objects . . . 45
Configuring User-Specified Response Objects . . . 47
Configuring Log Evidence Response Objects . . . 49
Configuring Quarantine Response Objects . . . 50

Chapter 7: Defining Policy Deployment Objects

Overview . . . 51
What are Policy Deployment Objects? . . . 52
Creating a Policy Deployment Object . . . 53

Chapter 8: Defining Event Rules

Overview . . . 55
What is an Event Rule? . . . 56
Adding Event Rules . . . 58
Defining Event Filters in Event Rules . . . 60
Defining Source Addresses and Source Ports in Event Rules . . . 61
Defining Destination Addresses and Destination Ports for Event Rules . . . 63
Defining Responses in Event Rules . . . 65
Defining Advanced Filters for Event Rules . . . 66
Working with Event Rules . . . 67
Customizing the Event Rules Tab . . . 69

Chapter 9: Defining Component Rules

Overview . . . 71
What is a Component Rule? . . . 72
Creating Component Rules . . . 73

Chapter 10: Defining Network Objects

Overview . . . 77
What are Network Objects? . . . 78
Defining Address Names in Network Objects . . . 80
Defining Address Groups in Network Objects . . . 82
Defining Port Names in Network Objects . . . 84
Defining Port Groups in Network Objects . . . 86
Defining Dynamic Address Names in Network Objects . . . 88
Exporting and Importing Network Objects Data . . . 90

Part III: Configuring Site-Level Policies and Responses

Chapter 11: Configuring Site-Level Policies

Overview . . . 93
What Are Policies? . . . 94
Configuring Custom Policies . . . 96
Applying Policies to Individual Agents . . . 97
Applying Policies to Groups . . . 98
Applying Policies with Policy Subscription Groups . . . 100
Working with Policies for Desktop Protection Agents . . . 103
Granting Users Permission to Modify Site-Level Policies . . . 104
Policy Assignment with Active Directory . . . 105

Chapter 12: Configuring Site-Level Responses

Overview . . . 107
What Are Responses? . . . 108
Configuring Custom Agent Responses . . . 111
Granting Users Permission to Modify Site-Level Responses . . . 112

Preface

Overview

Introduction

The *SiteProtector Policies and Responses Configuration Guide* contains information about configuring, updating, and maintaining policies and responses for SiteProtector.

Scope

This guide explains how to manage policies in SiteProtector using the Policy view, as well as how to manage policies at the Site level for certain agents. It also explains using Central Responses to alert security managers and analysts when events occur in your Site, or when SiteProtector components change status. Before you begin, you must have installed SiteProtector and any components that support agents and appliances. (See the *SiteProtector Installation Guide*.)

Audience

This guide is written for security managers who configure, update, and maintain policies and responses for SiteProtector. For many sites, the Security Manager is responsible only for maintaining the security of the network. For other sites, the Security Manager is also responsible for aspects of network and security administration, such as network administration and security analysis.

What's new in this guide

This guide is updated to include information about Service Pack 7.0. Service Pack 7 introduces a completely new methodology for managing policies in the Policy view. The Policy repository stores policies by unique name and maintains all past versions of policies as you make changes to them. The policies are still hierarchical, but you can deploy a policy to any group, sub-group, or individual agent that uses that repository. You can create multiple repositories at the group level, though most Sites should need only the default repository.

The Central Responses feature contains a new type of response object. Policy Deployment objects allow you to deploy a policy to certain agents when an event or component status matches your response rule.

How to Use SiteProtector Documentation

Using this guide

Use this guide to configure and maintain policies and responses for SiteProtector and for the agents that report to SiteProtector. When you configure SiteProtector the first time, follow the process described in the *SiteProtector Configuration Guide*, and use this guide for the Policy Configuration stage. After you have configured your system, use this guide to maintain policies and response settings.

Assumptions

The following assumptions may affect the procedures in this document:

- Some procedures may vary slightly depending on your operating system. The procedures in this guide are based on Microsoft Windows 2000 unless otherwise noted.
- When a procedure references an installation folder, it refers to the default installation folder. If you used a different folder, you must adjust the procedure accordingly.

User role

You must be assigned to the SiteProtector Administrator user role to perform most of the tasks in this guide.

Related publications

Use the following documents if you have not yet installed SiteProtector and need information about SiteProtector configuration options:

- *System Requirements*
- *Scalability Guide*
- *Supported Agents and Appliances*

Other SiteProtector user documents

Table 1 describes other SiteProtector user documents:

Document	Contents
SiteProtector Installation Guide	Provides the tasks for installing SiteProtector components and optional modules. It includes information about advanced configuration tasks such as hardening third-party software security, securing database communication, configuring firewalls for SiteProtector traffic, and configuring failover Event Collectors.
SiteProtector Configuration Guide	Provides the tasks for configuring the SiteProtector components after you install the SiteProtector application.
SiteProtector User Guide for Security Analysts	Provides background information, procedures, and recommendations for using SiteProtector to assess vulnerabilities and monitor and analyze suspicious activity on your network.
SiteProtector Help	Contains all the procedures that you need to use SiteProtector, including advanced procedures that may not be available in a printed user document.

Table 1: *Description of SiteProtector user documents*

Licensing Agreement

For licensing information on IBM Internet Security System products, download the IBM Licensing Agreement from:
http://www-935.ibm.com/services/us/iss/html/contracts_landing.html

Getting technical support

Introduction

IBM Internet Security Systems provides technical support through its Web site and by e-mail or telephone.

The IBM ISS Web site

The Customer Support Web page (http://www.ibm.com/services/us/iss/support/) provides direct access to online user documentation, current versions listings, detailed product literature, white papers, and the Technical Support Knowledgebase.

Hours of support

The following table provides hours for Technical Support at the Americas and other locations:

Location	Hours
Americas	24 hours a day
All other locations	Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding IBM ISS published holidays **Note:** If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.

Table 2: *Hours for technical support*

Contact information

For contact information, go to the Contact us section of the Customer Support Web page at http://www.ibm.com/services/us/iss/support/.

Part I

Managing Policies in the Repository

Chapter 1

Introduction to Policy Management

Overview

Introduction

Use the Policy view to create, edit, and deploy policies to agents or groups in SiteProtector.

When you deploy a policy to an agent, it becomes the active policy for the agent. SiteProtector components and other IBM Internet Security Systems agents come with default policies. You can customize these policies in SiteProtector, as well as create new policies for any of your agents.

In this chapter

This chapter contains the following topics:

Topic	Page
The Policy View	12
Upgrading from SP 6.1 to SP 7.0	13
Policy Permissions	15

The Policy View

Introduction

In the policy view, you can see where policies are deployed to and where they are inherited from. You can create, edit, and deploy policies. You can also import policies from agents that are configured locally and manage them in SiteProtector.

Four policy views

There are four areas available on the left pane of the Policy view. The following table describes the available options according to which node you select:

Node selected	Policy view
Groups and Agents	Selecting a group or agent in the left pane displays the policies currently deployed to agents in that group and allows you to configure policy inheritance for your Site. The Inherited From column shows the policy hierarchy for the group or agent you select. The Deployment Jobs pane displays information about when policies were deployed, as well as scheduled policy deployments for this group. **Tip:** Expand the **Policy Types Not Deployed** list to see available policies for the selected agent type and version that have not been deployed to this group. For more information, see “Working with Policies at the Group Level” on page 27.
Policy Repository	Selecting the Policy Repository displays all available policies for the Agent type selected. From here, you can create, edit, and deploy policies. For more information, see “The Policy Repository” on page 17.
Shared Objects	Selecting Shared Objects displays global objects that can be shared among multiple agents or groups in your Site. Fore more information, see “Shared Objects” on page 20.
Locally Configured Agents	Selecting Locally Configured Agents displays a list of agents using policies deployed outside of SiteProtector. This is a temporary access point for agents whose local policies have not yet been imported into SiteProtector. You must move agents out of this node to deploy policies to them from the Policy Repository. For more information, see “Locally Configured Agents” on page 31.

Table 3: *Four areas of Policy view*

Upgrading from SP 6.1 to SP 7.0

Introduction

SiteProtector Service Pack 6.0 and 6.1 users will notice many changes to the policy management methodology in Service Pack 7.0. SiteProtector now uses a true repository to store policies by name, keep a backup of all previous versions of those policies, and handle all deployment to groups and agents. Groups and agents still inherit policies from their parent groups, but it is now automatic, and inheritance management has changed. For more information on these changes, see Chapter 2, "The Policy Repository" and Chapter 3, "Working with Policies at the Group Level."

For more about new features in Service Pack 7.0, click **Help→What's New** in the SiteProtector Console.

Migrating policies

Most of the policies used in your SP 6.x Site will be added to the default repository when you perform the SP 7 upgrade. They will be added to the default repository with the name of the agent or group they belonged to as the new policy name. They will be automatically deployed to the same agents or groups as they were in SP 6.x.

Shared policies or policies using Shared Objects that are defined in groups other than the Site Group in SP 6.x will migrate to a new repository in the group where they are defined. If you have Shared Objects defined at the agent level, the agents will migrate to the Locally Configured Agents node.

Merging Shared Objects

Certain policies that contain information that can be used by multiple agents or multiple versions of the same agent are called Shared Objects. Because a policy repository contains only a single set of Shared Objects, you should define these Shared Objects only in the Site Group of your SP 6.x Site before you upgrade to SP 7.

If you continue the update process with any of these policies defined at a lower level than the Site Group, SiteProtector will create an additional policy repository for each group where these objects are defined. If you then want to use policies from the same repository on multiple groups, you must merge these repositories and consolidate the Shared Objects.

See also, “Shared Objects” on page 20, and “Working with Multiple Repositories” on page 19.

Locally Configured Agents

The Locally Configured Agents node is designed to be a temporary access point for agents whose local policies have not yet been imported into SiteProtector. You must move agents out of this node to take advantage of the policy features available in SiteProtector. You can import the agent's policies to use in SiteProtector or move the agents and use policies from the SiteProtector repository.

For more information on the Locally Configured Agents node, see “Locally Configured Agents” on page 31.

Where your 6.x policies go in 7.0

The following table describes what happens to your policies when you upgrade from SP 6.x to SP 7.0:

This policy in SP 6.x	Does this in SP 7.0:
Standard policy overridden at group “X” in “Deployed” policy repository	Policy named “X” in nearest parent repository and deployed to group “X”
Standard policy overridden at agent “Y” in “Deployed” policy repository	Policy named “Y” in nearest parent policy repository and deployed to agent “Y”
Standard policy overridden at group “X” in non-deployed policy repository	Policy named “A_X” in Default Repository
Standard policy overridden at agent “Y” in non-deployed policy repository	Policy named “A_Y” in Default Repository
Shared Object policy overridden at Site group “Deployed” policy repository	Shared Object policy belonging to Default Repository
Shared Object policy overridden at group “X” in “Deployed” policy repository	Policy repository created for group “X” containing the Shared Object
Shared Object policy overridden at agent “Y” in “Deployed” policy repository	Agent “Y” moved to Locally Configured Agents and uses copies of all pre-upgrade policies
Shared Object policy in any non-deployed policy repository	Discarded in SP 7.0

Table 4: *Policy placement in SP 7.0 upgrade*

Policy Permissions

Introduction

This topic provides information about the permissions needed to create, edit, and deploy policies in SiteProtector.

Deploy Policy permission

Permissions to deploy policies are set at the group level. So, if a user has the Deploy Policy permission for a group, he or she can deploy policies to, or remove deployments from, that group. Group permissions are hierarchical, so if you grant Deploy Policy permissions to a group, that user or user group will have the same permissions in all subgroups unless you set different permissions specifically for that subgroup.

Assigning Deploy Policy permissions

To grant Deploy Policy permissions for a user or group of users:

1. Select a group, and then click **Object→ Properties**.
2. Click the **Permissions** icon.
3. In the Users and/or Groups section, select the user or user group you want to assign Deploy Policy permissions.
4. For the Deploy Policy permission, click the circle in the **Control** column.
   - A black circle indicates that the user or user group can deploy policies to this group.
   - A white circle indicates that the user cannot deploy policy to this group.
5. Click the **Save** icon.

Modify policy permissions

Permissions to edit, create, and delete policies are set by agent type. They are also at the group level, but since all policies reside in the repository, permissions must be set for the group that contains the repository they reside in. For example, you can assign permissions to one user group to modify Network IPS policies, but not to modify Proventia Desktop policies in the same repository. If you use multiple repositories, you could also grant a user or user group permissions to modify Network IDS policies in one group's repository, but not in another.

Control policy permissions

The Control permission allows users or user groups to assign policy subscription groups to an agent type. They are also set for the group containing the repository they reside in. For example, you can assign permissions to one user group to change policy subscription groups for Network IPS agents, but not for Proventia Desktop agents.

Note: Network Enterprise Scanner has several policy types that also allow a View permission. For more information, please see the Enterprise Scanner documentation.

Shared policy types

Some policies are shared by different agent types. A user with permissions to a shared policy type for one agent can edit that policy for all agent types.

Example: The Group Settings policy is a shared policy. If you try to access Group Setting Policy from a repository in which you have Modify permissions for at least one of the following agents, you are allowed access:

- RealSecure Desktop
- Network Multi-Function Security

- X-Press Update Server
- Network IPS
- Event Archiver
- Proventia Server for Linux
- Proventia Server for Windows

Note: You are not allowed access if you do not have Modify permissions for at least one of these agents.

Assigning Modify or Control policy permissions

To grant users or user groups permissions to modify policies for an agent type:

1. Select a group, and then click **Object→ Properties**.
2. Click the **Permissions** icon.
3. In the Users and/or Groups section, select the user or user group you want to assign the permissions.
4. Expand the Agent type for which you want to grant permissions.
5. In the Policy permission section, click the circle in the **Modify** or **Control** column.
6. Click the **Save All** icon.

Chapter 2

The Policy Repository

Overview

Introduction

Use the policy repository to create, edit, and deploy policies in SiteProtector. The repository keeps an archive of each saved version of your policies.

In this chapter

This chapter contains the following topics:

Topic	Page
What is the Policy Repository?	18
Working with Multiple Repositories	19
Shared Objects	20
Managing Policies in the Repository	21
Importing and Exporting Policies	23
Policy Deployment	24
Migrating agent policy versions	26

What is the Policy Repository?

Introduction

The policy repository is a central archive of all the policies you create and use in your Site. Each time you edit a policy, SiteProtector saves a new version in the repository. You can deploy any version of a policy to an agent or group in your Site.

What you see

The top pane of the repository window displays all of the policies in your repository for the selected agent type and version. A list of policies that you have not created for that agent type and version appear in the **Policy Types Not Created** list. You can create these policies by clicking **New→ Policy**. The bottom pane of the repository displays the version history of the policy you select.

Working with Multiple Repositories

Introduction

You can use the default repository in SiteProtector to manage all of your policies or create additional repositories to separate different types or groups of policies.

Most Sites should need only the default repository to manage and deploy policies. Users who would want to use multiple repositories include providers of managed security services who manage Sites for multiple locations or businesses and need unique sets of policies and Shared Objects for each entity.

Creating a new repository

You can create a new repository only on a group with no active policy deployments.

To create a new repository:

1. Select a group for which to create the new repository, and then click **Object→New → Policy Repository**.
2. Click **Yes** on the confirmation box.
3. To copy policies from another repository, drag and drop them from that repository's list into the new repository.

Merging repositories

If you have created additional policy repositories in individual groups, you can merge them into the parent repository to consolidate and simplify the deployment process. Merging a repository copies all unique policies from the merged repository into the parent repository. Policies with identical names, as well as shared objects, are merged. This means that all unique attributes of the policy or object will be added to a single policy or shared object in the parent repository. Attributes that have the same name but are not identical will cause conflicts.

Important: You must resolve all conflicts for merged policies or shared objects to complete the repository merge.

To merge a policy repository into its parent repository:

1. Select **Policy** from the **Go to** list.
2. Select the repository you want to merge, and then click **Action→Merge**.
3. Click **OK** on the confirmation window.
4. If there are conflicting attributes in your policies or shared objects:
   - If you are merging policies with the same name that are not identical, the policy is automatically renamed by appending the name of the merged repository to the front of the policy name.
   - If you are merging shared objects with conflicting attributes, you must delete the conflicting attributes.

     Important: Each repository can contain only one set of shared objects. If you need multiple sets of shared objects, you must use more than one repository.
5. After you have resolved all conflicts, click **OK**.

Shared Objects

Introduction

Shared objects are policies that contain information that is used by multiple agents or multiple versions of an agent. A policy repository can only contain one of each type of Shared Object. The following policies reside in the Shared Objects node:

Shared Object	Agents used by
Network Objects	Event Archiver, Network Multi-Function Security, Network IPS, Proventia Server for Linux
Response Objects	Central Responses[a], Network IDS
Network Locations	Network Enterprise Scanner
Policy Objects	Proventia Network Mail Security
Global Tuning Parameters	Network IDS, Network IPS
Protection Domains	Network IDS, Network IPS
Notifications	Network Multi-Function Security, Proventia Network Mail Security
Global Actions	Proventia Desktop (7, 8, 9)

Table 5: *Shared Objects*

a. Central Responses use only Network Objects that reside in the default repository.

Managing Policies in the Repository

Introduction

Use the policy repository to create, edit, and delete policies in your Site. You can create a new policy from a blank template or by deriving a new file using information from an existing policy in your Site. You can create new versions of a policy by editing an existing policy.

Creating a new policy

To create a new policy based on the default policy for an agent:

1. Select **Policy** from the **Go to** list to open the Policy view, and then select the repository.
2. Click **New→Policy**.
3. Type a **Name** for the new policy.
4. To open a blank policy template, select **Generate Empty**, and then select a **Policy Type** from the list.
5. To import a policy file, select **Import from File**, and browse to the file you want to import.
6. Click **OK**.

Deriving a new policy from an existing policy

To derive a new policy from an existing policy:

1. Select **Policy** from the **Go to** list to open the Policy view, and then select the repository.
2. Select the policy you want to copy, and then click **Action→Derive New**.
3. Type a **Name** for the new policy, and then click **OK**.
4. Add or edit policy settings as needed, and then click **Action→Save Policy**.
5. If you want to schedule this policy to deploy to an agent or group, select the **Deploy this New Version** check box.

   Tip: For information on deploying policies, see "Policy Deployment" on page 24.
6. Click **OK**.

Editing a policy

Each time you edit a policy, a new version is stored in the repository.

To edit a policy:

1. Select **Policy** from the **Go to** list to open the Policy view, and then select the repository.
2. Select the policy you want to edit, and then click **Object→Open**.
3. Add or edit policy settings as needed, and then click **Action→Save Policy**.

Note: SiteProtector does not automatically deploy the updated policy. You must deploy the new version of the policy to implement your changes.

Deleting a policy

You cannot delete a policy from the repository if you have deployed it anywhere in your Site.

To delete a policy from the repository:

1. Select **Policy** from the **Go to** list to open the Policy view, and then select the repository.
2. Select the policy you want to delete, and then click **Edit→Delete**.
3. Click **Yes** on the confirmation window.

Importing and Exporting Policies

Introduction

You can import and export default or custom policies and responses in the policy repository.

Example: You created a policy for a Network IPS appliance, and you want to import the policy into SiteProtector, so you can apply it to groups or other appliances. Likewise, if you created a policy for a group in SiteProtector, you could export the policy to your Network IPS appliance.

Importing a policy

To import a policy into the repository:

1. Select **Policy** from the **Go to** list to open the Policy view, and then select the repository.
2. Click **Action→Import**.
3. Navigate to the policy you want to import, and then click **Import**.

Exporting a policy

To export a policy to use with an agent outside of SiteProtector:

1. Select **Policy** from the **Go to** list to open the Policy view, and then expand the repository.
2. Select the policy you want to export, and then click **Action→Export**.
3. Navigate to the location you want to save the file, and then click **Export**.

   Tip: You can change the name of the file when you export it.

Policy Deployment

Introduction

After creating or editing a policy, you must deploy it to the appropriate agents or groups.

Note: To modify policies for agents that you deployed outside of SiteProtector, you may need to import the policy into SiteProtector first.

Deploying a policy to a specific agent or group overrides policy inheritance from the parent group. Removing the specific policy deployment allows the group or agent to inherit the policy from its parent group again. For more information on inheritance, see "Policy Subscription Groups" on page 30.

Note: For performance reasons related to the quantity of agents typically used for those agent types, you cannot deploy policies directly to certain agents. For the following agents, you must deploy policies to the group containing the agent:

- Proventia Desktop
- Proventia Server for Windows
- Proventia Server for Linux

Deploying a policy

To deploy a policy from the repository:

1. Do one of the following:
   - Drag the policy icon from the repository to a group or agent in the left pane.
   - Select the policy icon in the repository, and then click **Action→ Deploy**.

   The Deploy Policy window displays the policy you chose, and the target(s) it will be deployed to.
2. To deploy additional policies, click the **Policies** icon, and then click **Add** to select more policies.
3. Click **OK**.
4. To select a target to deploy the policy to, click the **Targets** icon, and then select the groups or agents to deploy this policy to.
5. Click the **Schedule** icon.
6. To deploy the policy immediately, select **Now**.
7. To schedule a specific date and time to deploy the policy, select **Start Time**, click the drop-down list, and then select a date and time for deployment.
8. To prompt agents to update their policy immediately upon deployment, click the **Summary** icon, and then select the **Force affected components/appliances to contact SiteProtector when deployment completes** check box.
9. Click **OK**.

Removing a policy deployment

To remove a policy deployment from a specific agent or group:

1. Select **Policy** from the **Go to** list to open the Policy view.
2. Select the group or agent in the left pane, and then select the policy to remove.
3. Click **Action→ Remove Deployment**.

4. To remove additional policy deployments, do the following:
   - Click the **Policies** icon, and then click **Add**.
   - Select additional policies, and then click **OK**.
5. To remove the policy from multiple groups or agents, click the **Targets** icon, and then select additional groups or agents.
6. Click the **Schedule** icon.
7. To remove deployment immediately, select **Now**.
8. To schedule a specific date and time to remove the deployment, select **Start Time**, click the drop-down list, and then select a date and time to remove deployment.
9. To prompt agents to update their policy immediately upon removal, select the **Force affected components/appliances to contact SiteProtector when deployment completes** check box.
10. Click **OK**.

Viewing policy usages

You can use the Show Usages command to identify other groups and agents to which a particular policy is deployed.

To view policy usages:

1. In the policy repository, right-click a policy, and then select **Show Usages**.
   The **Deployed** tab displays the following information:

Option	Description
Target	The groups or agents to which this policy version is deployed
Deployment Time	The date and time the policy was deployed to each target
Deployment By	The SiteProtector user who last deployed the policy to each target

2. Click the **Scheduled** tab to see deployments that are scheduled but not yet complete:

Option	Description
Target	The groups or agents this policy is scheduled to be deployed to or removed from
Action	The scheduled action: deployment or remove deployment
Deployment Time	The time the deployment or removal is scheduled
Deployment By	The SiteProtector user who scheduled the action

3. Click **OK** when you are finished.

Migrating agent policy versions

Introduction

If you have upgraded some of your Proventia appliances and you want to use the same policies you defined for your older appliances, you can migrate the older, incompatible versions of your policies to the new version. You can migrate settings only at the group level; you cannot migrate policies directly for a single appliance.

Note: If you edit policies on the older appliance after you have migrated the policies to the new appliance, you must migrate the policies again for the newer appliance to have the updated versions.

Procedure

To migrate agent policies:

1. Select the group that contains the upgraded appliances, and then click **Action→ Updates→ Migrate Agent Version**.
2. Select the **Agent Type** from the list.
3. Click the **Upgrade Details** icon, and then select the older appliance version from the **Migrate From Firmware Version** list.
4. Select the new appliance version from the **Update to Firmware Version** list.
5. If the version to which you are migrating can update itself, select the **Update Agents** check box, and then select a date and time.
6. To prompt agents to update immediately, select the **Force affected agents to heartbeat** check box.
7. Click **OK**.

Chapter 3

Working with Policies at the Group Level

Overview

Introduction

This chapter provides information about what appears in the Policy view when you select a group or agent in the left pane. Although most policy deployment functions are done through the repository, you can still select groups and agents to see which policies are deployed there, where they are inheriting them from, and to which policy subscription groups your agents are assigned.

Note: Although some of the same policy functions are available at the group level, you should use the repository view to create and manage your policies. See "Managing Policies in the Repository" on page 21.

In this chapter

This chapter contains the following topics:

Topic	Page
Viewing Policy Deployments	28
Policy Inheritance	29
Policy Subscription Groups	30

Viewing Policy Deployments

Introduction

When you select a group or agent in the Policy view, the top pane displays details about the policies, based on the agent type and version selected, that are currently deployed to that group or agent. This includes the name and version of the policy deployed, as well as the parent group from which it is inherited.

Policies not deployed

You can expand the **Policy Types Not Deployed** list to see other available policies for the selected agent type and version that have not been deployed to this group. You can edit and deploy those policies from the repository.

Deployment history

The **Deployment Jobs** pane displays information about when selected policies were deployed, as well as scheduled policy deployments for this group.

Policy Inheritance

Introduction

As in previous versions of SiteProtector, groups and agents inherit policies from their parent groups. However, inheritance now happens automatically, and commands such as "Override" and "Promote" are no longer applicable.

When you select a group or agent in the Policy view, the Inherited From column displays the group where listed policies originate.

How policy inheritance works

Policy inheritance is similar to Windows file permissions in that it allows you to reuse a policy without having to redefine it at each level in the tree.

Agents and assets automatically inherit policy settings from the groups they reside in. These groups automatically inherit policy settings from the next higher group in your Site structure. A child agent or group that inherits policy from a parent group continues to use this policy until you either specifically deploy the policy at the child agent or group level, or you move the parent or child group to a location that is outside its current hierarchy.

Overriding inheritance

You can override policy inheritance by applying policy to individual agents, groups, or subgroups. Simply deploy a different policy to the specific subgroup or agent, and that policy is no longer inherited from the parent group.

To remove the overriding policy, simply remove the deployment from the subgroup agent, and the agent or group will automatically inherit the policy from its parent group.

Note: For instructions on deploying and removing policies, see "Policy Deployment" on page 24.

Policy Subscription Groups

Introduction

Use policy subscription groups to apply common policy settings to several agents in the same group.

What is a policy subscription group?

Although agents can reside in more than one group in your Site structure, an agent can subscribe to policies from only one group. In the policy view, an agent will appear in its policy subscription group.

Because policies can be set at the group level, you should create at least one policy subscription group for every unique policy that you plan to deploy. You can assign any folder in a Site as a policy subscription group, except the Unassigned Assets folder.

Note: Each group may have only one policy for each agent type.

Once you assign an agent or group to a policy subscription group, it automatically applies any policy changes made at the group level. Policy changes are automatically sent to most agents; Desktop agents receive policy updates the next time they send a heartbeat to the Agent Manager.

Assigning a policy subscription group

To assign a policy subscription group to an agent:

1. Select a group, and then select **Agent** from the **Go to** list to open the Agent view.
2. Select the agent, and then click **Action→Configure Agents→Assign Policy Subscription Group**.
3. Select a group in the tree.

   Important: If you select **None**, SiteProtector will move the agent outside of the grouping structure and the agent will not inherit policies from any group.
4. Click **OK**.

Chapter 4

Locally Configured Agents

Overview

Introduction

Agents whose policies are managed locally (using Proventia Manager) appear in the Locally Configured Agents node. You must move agents out of this node to take advantage of the policy features available in SiteProtector.

In this chapter

This chapter contains the following topics:

Topic	Page
Locally Configured Agents	32
Migrating Locally Configured Agents into SiteProtector	33

Locally Configured Agents

Introduction

The Locally Configured Agents node is designed to be a temporary access point for agents whose local policies have not yet been imported into SiteProtector. You should move these policies into the policy repository to manage them in SiteProtector.

You can import the agent's policies to use in SiteProtector or move the agents and use policies from the SiteProtector repository.

What is a locally configured agent?

A locally configured agent does not inherit policy from any group. It uses policies that reside on the agent itself, and cannot take advantage of the policy management features in SiteProtector.

If the agent has a policy subscription group, the agent name will appear in that group in the color gray, and also under the Locally Configured Agents node. After you migrate the agent into the Repository, it resides in its assigned policy subscription group.

How do my agents get there?

Agents are placed in the Locally Configured Agents node when they are added to your Site, but you do not migrate their policies into SiteProtector. This often happens when you upgrade from SiteProtector Service Pack 6.x to Service Pack 7.0. You can edit the agent's policies in SiteProtector, as well as on the agent itself, but you cannot use these policies for other agents in your Site.

Migrating Locally Configured Agents into SiteProtector

Introduction

You must migrate agents out of the Locally Configured Agents node to take advantage of the policy features available in SiteProtector.

Procedure

To migrate locally configured agents:

1. Select **Policy** from the **Go to** list to open the Policy view, and then select **Locally Configured Agents**.
2. Select the agent, and then click **Action→Migrate to Repository**.
3. Select the **Import Policy** check box to import the agent's policies into the repository, and then select the policies you want to import.

   Important: If you select this option, the agent will not inherit the selected policies from its parent group. Any policies you do not select are deleted permanently.

   Note: Agent-specific policies are imported automatically.
4. Click **OK**.
   Any imported policies appear in the Repository and can be deployed to other groups or agents in SiteProtector.

   Attention: When you merge locally managed agent policies into the repository, not all policy settings will be migrated. Settings that are not list data (e.g. check boxes and text fields) will automatically inherit the values set for the policy in that repository. You should open and review the policy settings after the migration is complete to ensure that your policy settings are correct.

Part II

Configuring Central Responses

Chapter 5

Working with Central Responses

Overview

Introduction

This chapter provides an overview of the Central Responses feature in SiteProtector. Central Responses provide control over responses to events and the status of components in a central location in SiteProtector.

In this chapter

This chapter contains the following topics:

Topic	Page
What are Central Responses?	38
Creating Central Responses	39

What are Central Responses?

Introduction

The Central Responses feature allows you to create response rules that apply to events or component statuses that occur in your Site.

If event parameters match a response rule you create, SiteProtector generates a notification in the form of an e-mail, SNMP, or user specified response. You can control how often this notification is generated and on what event parameters it is based.

Components of Central Responses

A central response comprises a Response Rule and a Response Object. The Response Rule determines when a response is initiated. The Response Object is the action taken when the rule is triggered. In addition, you can create Network Objects, which are defined segments of your network that you can reuse throughout multiple responses.

The following table describes the three components of Central Responses:

Component	Description
Response Rule	Defines the criteria required to generate a response.
Response Object	Defines a particular response, such as an e-mail to one or more individuals. You assign response objects to response rules to define the response to generate for each rule. There are six types of response objects: • E-mail • SNMP • Log Evidence • Quarantine • User-specified
Policy Deployment Object	Policy Deployment Objects are a special type of response that deploy pre-configured policies to groups or agents in your Site when criteria for a Response Rule is met.
Network Object	Network Objects define custom network address and port lists that policies and responses can share. You can assign network objects to rules to define which assets the rule covers. **Note:** Network objects are optional. You can also define specific assets in the response rule.

Table 6: *Components of Central Responses*

Creating Central Responses

Introduction

Central Responses use a rule (Response Rules) to apply responses (Response Objects or Policy Deployment Objects) to assets or agents in your Site (Network Objects). However, when creating Central Responses, you may find it easier to build them in the reverse order.

Building from the ground up

Response Rules include both the Response Object (or Policy Deployment Object) that is applied by the rule, as well as the location where the Object is applied (which can be a Network Object). Therefore, it makes sense to create any Network Objects and Response Objects you want to use before you create the Response Rule.

Procedure

To create Central Responses:

1. Select **Tools→Central Responses** to open the Central Responses window.
2. Define any Network Objects you want to use.
3. Define the Response Object or Policy Deployment Object you want to apply.
4. Define the Response Rule to trigger the response.

Chapter 6

Defining Response Objects

Overview

Introduction This chapter provides information about defining Response Objects.

In this chapter This chapter contains the following topics:

Topic	Page
What are Response Objects?	42
Configuring E-mail Response Objects	43
Configuring SNMP Response Objects	45
Configuring User-Specified Response Objects	47
Configuring Log Evidence Response Objects	49
Configuring Quarantine Response Objects	50

What are Response Objects?

Introduction

Response Objects capture information that SiteProtector uses when it responds to security events. For example, you can configure policies that require SiteProtector to send an e-mail to the Site administrator when a specific event occurs on your network. You can define an e-mail message as a Response Object. Response Objects are reusable, meaning that you can include information from a Response Object when you define several different Response Rules. This design eliminates the tasks of reentering the information each time you define a rule. It also provides a way to manage and update the information in a central location. When you update information in the Response Object, the information is automatically updated wherever the Response Object is used.

Policy information

Response Objects can include any of the following information:

- settings for e-mail responses
- settings for SNMP responses
- settings for user-specified responses
- settings for responses that log evidence (for Proventia Network IPS only)
- settings for responses that quarantine events (for Proventia Network IPS only)

Response Objects are stored in the Site Database.

Task overview

Table 7 describes the tasks for defining Response Objects:

Task	Description
1	Define e-mail addresses in the Response Object. See “Configuring E-mail Response Objects” on page 43.
2	Configure SNMP settings in the Response Object. See “Configuring SNMP Response Objects” on page 45.
3	Configure user-specified settings in the Response Object. See “Configuring User-Specified Response Objects” on page 47.
4	Configure log evidence settings (for Proventia Network IPS) appliance if necessary. See “Configuring Log Evidence Response Objects” on page 49.
5	Configure quarantine settings the Proventia Network IPS if necessary. See “Configuring Quarantine Response Objects” on page 50.

Table 7: *Tasks for defining Network Objects*

Configuring E-mail Response Objects

Introduction

This topic provides information about adding, removing, and editing e-mail Response Objects.

Description

E-mail Response Objects contain the information that SiteProtector sends in an e-mail message in response to a security event. You can define the following items that are included in the e-mail:

- name of the e-mail
- SMTP host
- from
- to
- subject
- body

Note: In the subject line and body of the e-mail, you can include parameters, such as the following:

- name of the agent that detected the event
- the destination address of the security event
- the port of the security event
- the address of the agent that detected the event
- the status of the agent that detected the event
- the version of the agent that detected the event

Adding e-mails

To add an e-mail address to the Response Object:

1. Click **Tools→Central Responses**, and then click **Response Objects**.
2. Select the **E-mail** tab, and then click the **Add** icon.

   Note: A red box indicates required information.
3. In the **Name** text box, type a name for the e-mail.
4. In the **SMTP Host** text box, type the IP address or DNS name of the SMTP host that handles the e-mail.
5. In the **From** text box, type the e-mail address from which the message originates.

   Note: You can only enter one From address. SiteProtector verifies that the From address is formatted correctly.
6. In the **To** text box, type the e-mail address(es) where the notification should be sent.

   Note: You can enter multiple addresses. Use semicolons to separate them.
7. In the **Subject** section, perform the following tasks as necessary:
   - Type a subject line for the e-mail.

- Select parameters from the **Agent Parameters** tree.

Note: When working with Central Responses, you should add parameters from the Common folder for Event Rules. You should add parameters from the Component folder when working with Component Rules.

8. In the **Body** section, perform the following tasks as necessary:
   - Type the body of the e-mail.
   - Select an item from the **Common Parameters** folder, and then click **Body**.

   Tip: Use text to label any common parameters selected. Otherwise, the parameter appears in the e-mail notification without reference to what the parameter represents.
9. Click **OK**, and then click **Apply**.

Editing e-mail addresses

To edit an e-mail address in the Response Objects policy:

1. Click **Tools→Central Responses**, and then click **Response Objects**.
2. Select the **E-mail** tab.
3. Select the e-mail response, and then click **Edit**.
4. Change the e-mail address as necessary, and then click **OK**.
5. Click **Apply**.

Removing e-mails

To remove an e-mail from the Response Objects policy:

1. Click **Tools→Central Responses**, and then click **Response Objects**.
2. Select the **E-mail** tab.
3. Select the e-mail response, and then click **Remove**.
4. Click **Yes** in the alert window to confirm your changes.

Configuring SNMP Response Objects

Introduction

This topic provides information about adding, removing, and editing SNMP Response Objects.

Description

An SNMP response is a response that SiteProtector sends to a SNMP manager. The response includes data from data from SNMP-compliant devices, called agents, about the following types of events:

- connection events
- user-defined events
- security events

Background

Simple Network Management Protocol (SNMP) is a set of protocols for managing networks. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return the data to SNMP management applications, such as OpenView. SNMP agents only communicate with SNMP management applications located in the same community. A community is a user-defined setting for basic authentication. The SNMP settings in the Response Objects policy define the IP address and community for the SNMP manager.

Note: The IBM ISS MIB file (iss.mib) defines the format of the SNMP traps and is used by SNMP management applications to provide a translation of the numeric Object Identifiers (OIDs) in the trap messages. To display the Event Name in SNMP trap messages, import or compile iss.mib in a SNMP management application. You can download the iss.mib file from www.iss.net/download.

Adding SNMP response

To add an SNMP response to the Response Objects policy:

1. Click **Tools→Central Responses**, and then click **Response Objects**.
2. Select the **SNMP** tab, and then click the **Add** icon.
3. Type a name for the SNMP response.
4. In the **Manager** text box, type the IP address to which the trap is sent.
5. In the **Community** text box, type a valid name used to authenticate with the SNMP agent.
6. Click **OK**, and then click **Apply**.

Editing SNMP response

To edit an SNMP response in the Response Objects policy:

1. Click **Tools→Central Responses**, and then click **Response Objects**.
2. Select the **SNMP** tab, and then select the SNMP response.
3. Change the setting as necessary, and then click **OK**.
4. Click **Apply**.

Removing SNMP response

To remove an SNMP response from the Response Objects policy:

1. Click **Tools→Central Responses**, and then click **Response Objects**.
2. Select the **SNMP** tab.
3. Select the SNMP response, and then click the **Remove** icon.
4. Click **Yes** in the alert window to confirm your changes.

Configuring User-Specified Response Objects

Introduction

This topic provides information about adding, removing, and editing user-specified Response Objects.

Important: The user-specified response must be compatible with Windows-based applications.

Description

A user-specified response is a custom response that SiteProtector generates when an event occurs. The response can include any of the following actions:

- start an application
- run a script
- run other commands

Requirements

The following requirements apply to user-specified responses:

- The response must be supported on Windows-based applications.
- Scripts must be stored on the Application Server computer.
- Responses must include the complete path to the storage location on the Application Server.

Adding a user-specified response

To add an user-specified response to the Response Objects policy:

1. Click **Tools→Central Responses**, and then click **Response Objects**.
2. Select the **User-Specified** tab, and then click **Add**.
3. In the **Name** text box, type a name for the user specified response object.
4. In the **Command** text box, type a command associated with the user-specified response object.

   Note: Include the complete path, including the drive, to the command script or executable response located on the Application Server.
5. Select parameters from the **Agent Parameters** tree.

   Note: When you work with Central Responses, you should add parameters from the Common folder for Event Rules. When you work with Component Rules, you should add parameters from the Component folder.
6. Use the **Remove**, **Move Up**, and **Move Down** options to arrange the parameters.
7. Click **OK**, and then click **Apply**.

Editing a user-specified response

To edit a user-specified response in the Response Objects policy:

1. Click **Tools→Central Responses**, and then click **Response Objects**.
2. Select the **User-Specified** tab.
3. Select the response, and then click **Edit**.
4. Change the response as necessary, and then click **OK**.
5. Click **Apply**.

Removing a user-specified response

To remove a user-specified response in the Response Objects policy:

1. Click **Tools→Central Responses**, and then click **Response Objects**.
2. Select the **User-Specified** tab.
3. Select the response, and then click **Remove**.
4. Click **Yes** in the alert window to confirm your changes.

Configuring Log Evidence Response Objects

Introduction

This topic provides information about configuring log evidence Response Objects.

Important: These settings control the behavior of the Network IPS appliance only.

Description

Log evidence allows you to configure the appliance to log the summary of an event. The Log Evidence response creates a copy of the packet that triggers an event and also records information that identifies the packet, such as Event Name, Event Date and Time, and Event ID. Evidence logs show you what an intruder attempted to do in your network.

Procedure

To configure a Proventia Network IPS Log Evidence Response Object:

1. Click **Tools→Central Responses**, and then click **Response Objects**.
2. Select the **Log Evidence** tab.

   Note: The Log Evidence tab displays the Proventia G default log evidence settings. You can modify these settings to meet your security requirements.
3. In the **Maximum Files** text box, type the maximum number for log evidence files.

   Note: When the log reaches the maximum number of files, it begins again with 0 and overwrites the existing files.
4. In the **Maximum File Size** text box, type the maximum file size of the log evidence files.
5. In the **Log File Prefix** text box, type a name for the log evidence file.
6. In the **Log File Suffix** text box, type the file extension for the log evidence file.
7. Click **OK**.
8. Click **Apply**.

Configuring Quarantine Response Objects

Introduction

This topic provides information about configuring quarantine Response Objects. The Proventia Network IPS can *quarantine* persistent attacks.

Important: These settings only control the behavior of the Proventia Network IPS.

Default settings

Table 8 describes the default quarantine settings in the Response Object:

Quarantine Setting	Description
Quarantine Intruder	Blocks reoccurring targeted attacks and both the computers (the victim computer and the intruder computer) involved in an attack.
Quarantine Trojan	Prevents attackers from regaining access to a computer that is infected with an open back door Trojan, such as Back Orifice.
Quarantine Worm	Blocks automated worms, such as Sasser, when a source is attacking your network.

Table 8: *Default quarantine settings in Response Objects*

Note: You *cannot* rename or remove the default quarantine settings.

Attention: Applying quarantines that you created can have negative results on your system. Be sure to familiarize yourself with how the quarantine process works before you apply a user-created quarantine. You should use the default quarantine settings because these settings will work in most cases.

Procedure

To define a Quarantine Response Object:

1. Click **Tools→Central Responses**, and then click **Response Objects**.
2. Select the **Quarantine** tab, and then click **Add**.

   The Add Quarantine window appears.
3. Type a name for the quarantine setting.
4. Select the following options as necessary:
   - **Victim Address**
   - **Victim Port**
   - **Intruder Address**
   - **Intruder Port**
   - **ICMP Port**
   - **ICMP Code**
   - **ICMP Type**
5. Click **OK**, and then click **Apply**.

Chapter 7

Defining Policy Deployment Objects

Overview

Introduction

This chapter provides information about Policy Deployment Objects, a special type of response that deploys pre-configured policies to groups or agents in your Site when criteria for a Response Rule is met.

In this chapter

This chapter contains the following topics:

Topic	Page
What are Policy Deployment Objects?	52
Creating a Policy Deployment Object	53

What are Policy Deployment Objects?

Introduction

Policy Deployment Objects are a special type of response that deploy pre-configured policies to groups or agents in your Site when criteria for a Response Rule is met.

You can create policy deployment objects to instruct SiteProtector to apply pre-configured policies to IPS agents when certain agent events are detected.

Example

You create a policy deployment object to apply a Proventia IPS policy to block a specific worm. You then create a response rule that triggers your policy deployment object whenever that worm is detected. An ADS agent in your Site detects worm behavior and identifies a specific worm. The policy deployment object enables an IPS policy on your Proventia GX IPS that blocks that all known IRC-managed Trojans for the suspected infected host

Creating a Policy Deployment Object

Introduction

You must complete three steps to create a Policy Deployment Object:

- Configure Deployment Object settings
- Select a policy to deploy
- Select deployment targets

Configuring Deployment Object settings

To configure Deployment Object settings:

1. Select **Tools→ Central Responses**, and then click **Policy Deployment Objects**.
2. Do one of the following:
   - Click the **Add** icon.
   - Select an existing Deployment Object, and then click the **Edit** icon.
3. On the Event Driven Deployment window, click the **Setup** icon.
4. Type a unique **Response Name**.
5. Select the **Agent Type**, **Agent Version**, and **Agent Mode** for the agent policy you want to deploy.
6. If you are using multiple repositories, select the **Repository** that contains the policy you want to deploy.

Selecting a policy to deploy

After you configure basic Policy Deployment Object settings, select the policy you want to deploy when your Response Rule criteria is met.

To select a policy:

1. In the Event Driven Deployment window, click the **Policies** icon.
2. Click **Add**.
3. Select the policy you want to deploy, and then click **OK**.

Selecting deployment targets

After you select the Policy you want to deploy, select the groups or agents to which you want to deploy it.

To select deployment targets:

1. On the Event Driven Deployment window, click the **Targets** icon.
2. Select the groups or agents to which you want to deploy the policy, and then click **OK**.
3. Click **OK** to exit Central Responses.

Chapter 8

Defining Event Rules

Overview

Introduction

This chapter provides information about defining event rules, which are Response Rules based on events detected by the Event Collector.

In this section

This chapter contains the following topics:

Topic	Page
What is an Event Rule?	56
Adding Event Rules	58
Defining Event Filters in Event Rules	60
Defining Source Addresses and Source Ports in Event Rules	61
Defining Destination Addresses and Destination Ports for Event Rules	63
Defining Responses in Event Rules	65
Defining Advanced Filters for Event Rules	66
Working with Event Rules	67
Customizing the Event Rules Tab	69

What is an Event Rule?

Introduction

This topic provides information about event rules.

Definition

An *event rule* is a user-defined set of criteria that must be met before SiteProtector generates a response to an event. You can create up to 200 event rules.

Criteria include the following:

- the event name
- the source IP address associated with the event
- the source port associated with the event
- the destination IP address associated with the event
- the destination port associated with the event
- the responses that must be generated when the criteria are met
- the advanced parameters

Event rules can be as simple or as complex as needed to meet your specific security requirements. For example, you can define a single IP address or a range of IP addresses for the source or destination IP address. You can also define different responses for the same event. For example, you can require SiteProtector to send an e-mail and generate an SMNP response to a single event.

Examples

The following are examples of event rules:

- When *Event_Name* occurs on IP address **127.0.0.1** and targets IP address **192.0.2.0** one time in 60 seconds, SiteProtector must send an e-mail to the Site administrator that includes detailed information about the event.
- When any event occurs on any IP address within the range of **192.0.2.0**-**192.0.2.24** range, SiteProtector must respond with a user-specified response.
- When Event_Name occurs on port 339 on any IP address within the range of **192.0.2.0**-**192.0.2.24**, SiteProtector must generate an SMNP response.

Methods

Table 9 describes the methods for defining event rules in the Response Rules policy:

Method	Description
Automatic	From the Analysis view, you can select an event(s), and then run the *Add Response Rules Wizard* to define response rules based on the select event(s). **Note:** You can select up to 50 events for one rule. If you select more than 50 events, the Create Response Rule menu is not available. The advantage of this method is that it automatically includes information about the event in the rule, such as event name, source address, and destination address. The disadvantage of this method is that the event must enter the system before you can create a response rule for it.

Table 9: *Methods for creating response rules*

Method	Description
Manual	From the Policy view, you can edit the Response Rules policy to include new response rules. The advantage of this method is that you can create response rules at any time and before the events enter the system. The disadvantage of this method is that you must provide all required information for the event manually. If you do not have the required information, then you can use wildcards.

Table 9: *Methods for creating response rules (Continued)*

Restrictions

The following restrictions apply to response rules in the Response Rules policy:

- The policy can contain up to 200 individual response rules.
- Each individual response rule can be associated with up to 50 events.

Adding Event Rules

Introduction

This topic explains how to perform the following tasks:

- manually add an event rule
- run the Add Response Rules Wizard to automatically add an event rule

Required information

When you manually add an event rule, you must define the following information:

- the event, including event name, status, and priority

  See "Defining Event Filters in Event Rules" on page 60.
- the source IP address(es) and port(s) associated with the event

  See "Defining Source Addresses and Source Ports in Event Rules" on page 61.
- the destination IP address(es) and port(s) associated with the event

  See "Defining Destination Addresses and Destination Ports for Event Rules" on page 63.
- the response SiteProtector generates when an event matches the criteria specified in the event rule

  See "Defining Responses in Event Rules" on page 65.
- custom, user-defined parameters for the event rule

  See "Defining Advanced Filters for Event Rules" on page 66.

Manually adding event rules

To manually add an event rule:

1. Click **Tools→Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab, and then click **Add**.
3. The Add Event Rules window appears.
4. Select the **Enabled** check box.
5. Define the following fields:

Field	Description
Name	Provide a name of up to 50 characters in length for the event rule.
Comment	Provide a description for the event rule.
Rule Threshold	Select this option if you want to define how often the criteria in the event rule must be met before SiteProtector generates the response. **Example** Send a response if the rule is triggered one time in 60 seconds.

6. Complete the following tasks as necessary:

Task	Reference
Define event details on the **Event** tab.	See "Defining Event Filters in Event Rules" on page 60.

Task	Reference
Define source addresses and ports on the **Source** tab.	See “Defining Source Addresses and Source Ports in Event Rules” on page 61.
Define destination addresses and ports on the **Destination** tab.	See “Defining Destination Addresses and Destination Ports for Event Rules” on page 63.
Define the responses SiteProtector generates when an event matches the criteria specified in the event rule on the **Responses** tab.	See “Defining Responses in Event Rules” on page 65.
Define custom, user-defined parameters on the **Advanced Filters** tab.	See “Defining Advanced Filters for Event Rules” on page 66.

Automatically adding event rules

To add an event rule automatically with the Add New Response Rule Wizard:

1. In the left pane, select the Site Group.

   Note: Make sure you have **Show Subgroups** enabled to view all events in the Site.

2. In the **View** list, select **Analysis**.
3. In the **Analysis View** list, select **Event Analysis - Details.**

   Tip: Perform this procedure on the Event Analysis - Details view. If you perform this procedure on other Analysis views, then the Wizard cannot automatically populate all required fields in the event rule.

4. Select up to 50 events on which to base the response rule.
5. Right-click the selected event(s), and then select **New Response Rule** from the pop-up menu.

   The Add New Response Rule Wizard begins.

6. Type a **Name** for the response rule, and then click **Next**.

   The Event Rules tab appears with information about the event.

   Note: To edit the information, select the rule, and then click **Edit**.

7. Click **OK**.

Defining Event Filters in Event Rules

Introduction

As events occur on any sensor or appliance in your Site, they are matched to the rules that you have created. When an event matches a rule's criteria, SiteProtector determines if all the other parameters also match. If all parameters match the rule, SiteProtector generates a response.

Note: You can associate up to 50 events with each response rule.

Example

You may add an event to a rule that includes all HTTP events with a high priority. When an HTTP event with a high priority occurs, SiteProtector will generate a response.

Procedure

To define event filters in an event rule:

1. On the **Events** tab, click **Add**.
2. Select the **Enabled** check box.
3. Type the event name.

   Note: Users with ADS agents on their Site can click **Select Event** to select from a list of ADS events.

   Tip: The event name can include the asterisk (*) as a wildcard symbol. The following are examples of valid entries:

   - `http_get`
   - `*http*`
   - `*http`
   - `http*`
4. Select a priority for the event.

   The priority of the event must match the priority you select before SiteProtector generates a response.
5. In the Status section, select the **Enabled** check box beside the event status.

   The status of the event must match the status you select before SiteProtector generates a response.
6. Click **OK**, and then click **OK** again.
7. Click **Save All**.

Defining Source Addresses and Source Ports in Event Rules

Introduction

This topic explains how to define source addresses and source ports in event rules.

Purpose

The purpose of this procedure is to associate events with source addresses and ports. The event source address and port must match the information you specify in this procedure before SiteProtector generates a response.

About back door response events

If you use back door response events to set up a rule, and you specify source and/or destination IP addresses, the source and destination IP addresses will be reversed on the Sensor Analysis tab:

- The source IP address appears in the destination IP address column (or appears as the victim).
- The destination IP address appears in the source IP address column (or appear as the attacker).

Defining source addresses

To define a specific source IP address:

1. On the **Source** tab, select **Use specific source address.**
2. Select one of the following from the **Mode** list:

Option	Description
From	Select this option to *include* events from the IP addresses you specify.
Not from	Select this option to *exclude* events from the IP addresses you specify.

3. In the **Specific sources** section, select one of the following options:

Option	Action
Any	Select this option to include any IP address or port.
Single IP Address	Select this option to include a single IP address in the address name, and then do one of the following: • select the IP address in the list; this list includes addresses you defined in the Network Objects policy • click **Add**, and then add an address to the list
Network Address / #Network Bits (CIDR)	Select this option to include IP address and network mask in the address name, and then type the required information.
IP Address Range	Select this option to include an IP address range in the address name, and then type the IP address range.
IP Address List Entry	Select this option to include a list of IP addresses in the address name, and then do one of the following: • from the drop-down list, select the **Address Entry List Name** • click **Add Address Names**, and then add a name to the Network Object policy.

4. Click **OK**, and then click **Apply**.

Defining source ports

To define a specific source port in the event rule:

1. On the **Source** tab, select one of the following options in the **Source Port** section on the Source tab:

Option	Description
Any	Include all ports in your Site.
Single Port	Specify one port in your Site.
Port Range	Include a port range. Type the first and last ports in the range.
Port List Entry	Include a Network Object Port Name. Select it from the Port List Entry Name list. To create a new Port Name to include here, click **Add Port Name**. The Add Port Name window appears and enables you to create a new list entry.

2. Click **OK**, and then click **Apply**.

Defining Destination Addresses and Destination Ports for Event Rules

Introduction

This topic explains how to define destination addresses and destination ports in event rules.

Purpose

The purpose of this procedure is to associate events with destination addresses and ports. The event destination address and port must match the information you specify in this procedure before SiteProtector generates a response.

About back door response events

If you use back door response events to set up a rule, and you specify source and/or destination IP addresses, the source and destination IP addresses will be reversed on the Sensor Analysis tab:

- The source IP address appears in the destination IP address column (or appears as the victim).
- The destination IP address appears in the source IP address column (or appear as the attacker).

Defining destination addresses

To define a specific destination address:

1. On the **Destination** tab, select one of the following options in the **Destination Address** section:

Option	Description
Any	Include events from all IP addresses.
Single IP Address	Include events only from IP addresses you specify. **Tip:** Click **Add** to add single IP addresses to the list.
Network Address/ #Network Bits (CIDR)	Include an IP address on a subnet. Type the IP address and mask. The mask is the network identifier, and is a number from 1 to 32; for example: 192.0.2.0 / 24.
IP Address Range	Include an address range, and then type the first and last addresses in the range. Do not use 0.0.0.0-255.255.255.255 as the Site range. If you use this as the Site range, random IP addresses are added to your ungrouped assets folder, such as IP addresses from Web sites.
Address List Entry	Include a Network Object Address Name. Select it from the list. To create a new Address Name to include here, click **Add Address Name**. The Add Address Name window appears and enables you to create a new list entry.

Defining any destination port

To include any destination port in the event rule:

- Select the **Any** option on the **Destination** tab.

Defining a specific destination port

To define a specific destination ports in the event rule:

1. On the **Destination** tab, select one of the following options:

Select this option...	To do this...
Any	Include all ports in your Site.
Single Port	Specify one port in your Site.
Port Range	Include an port range. Type the first and last ports in the range.
Port List Entry	Include a Network Object Port Name. Select it from the Port List Entry Name list. To create a new Port Name to include here, click **Add Port Name**. The Add Port Name window appears and enables you to create a new list entry.

2. Click **OK**, and then click **Apply**.

Defining Responses in Event Rules

Introduction

When an event occurs that matches a response rule, SiteProtector can send an e-mail to a responsible party, such as an incident response team or a Site Administrator, it can generate an SNMP response, or it can run a user-specified script on the application server.

Note: The Response Frequency threshold is determined using the local time on your application server. If the local time on the application server is reset for any reason, response frequency may be met, and additional responses may be generated.

Procedure

To select a response:

1. On the Responses tab, select the **Response Frequency** check box, and then type or select the appropriate values for **Send at most** ***[n]*** **responses within** ***[n] [time period]***.

   Note: The default is one response within 60 seconds. If you do not specify a response frequency, then SiteProtector sends a notification every time the rule is matched.

2. Complete one or more of the following tasks:

   Note: You create the e-mail, SNMP, or user-specified responses that appear in **Response Rules** on the **Responses** tab. If you do not see the e-mail, SNMP, or user-specified information you want to associate with this rule in the list, click **Manage Responses** to add it to the list.

   - Select the **E-mail** tab, and then select the check box in the **Enabled** column for the e-mail response to associate with this rule.
   - Select the **SNMP** tab, and then select the check box in the **Enabled** column for the SNMP response to associate with this rule.
   - Select the **User-Specified** tab, and then follow the instructions for "Configuring User-Specified Response Objects" on page 47.

3. Select another tab to continue, or click **OK**.

Defining Advanced Filters for Event Rules

Introduction

This topic explains how to add advanced filters to an event rule.

Definition

An *advanced filter* is a attribute-value pairs (AVPs) used to define information about the event. Some AVPs are created for you automatically when you create the event rule. For example, when you create an event rule and specify 127.0.0.1 as the source IP address, an AVP is created for you automatically with the following attribute-value pair:

- the attribute (parameter) is SourceAddress
- the value is 127.0.0.1

You can add other AVPs for the event rule as necessary. For example, you can manually add AVPs for user name or sensor name.

Note: Some event details appear in the Analysis tab. This allows you to see the parameters/values that are available to you. After you create a rule using the Wizard, the values are automatically populated.

Guidelines

When creating AVPs, use the following guidelines:

- Attributes (parameters) should be unique.
- Wildcard characters are not allowed.
- Do not use any of the following because these attributes can be defined in the Events, Source, and Destination tabs:
  - AlertName
  - SourceAddress
  - SourcePort
  - DestinationAddress
  - DestinationPort

Procedure

To add an advanced filter to an event rule:

1. On the **Advanced Filters** tab, click **Add**.

   The Add window appears.
2. Select the **Enabled** check box.
3. Type a unique **Parameter** for the advanced filter without spaces.

   Example: UserName

   Note: Do not use wildcard characters or any of the following: AlertName, SourceAddress, SourcePort, DestinationAddress, or DestinationPort.
4. Type a **Value** for the advanced filter without spaces.

   Example: BobW

   Note: Do not use wildcard characters.
5. Click **OK**, and then click **Apply**.

Working with Event Rules

Introduction

This topic explains how to perform the following tasks in the Response Rules policy:

- enable and disable event rules
- edit event rules
- remove event rules
- ordering event rules

Rule order

SiteProtector implements event rules in the order you specify. The event rule's location in the list determines the order in which it is implemented. When you create new event rule, the rule is automatically positioned in the event rule list as follows:

- If you select an event rule before you create the new response rule, the new event rule is placed above the rule you selected.
- If no rule is selected at the time you create the event rule, the new event rule is placed in the last position in the list.
- If you use the Rule Wizard to create the event rule, the new event rule is placed at the first position in the rule list.

Enabling and disabling event rules

To enable and disable an event rules in the Response Rules policy:

1. Click **Tools→Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab.
3. Select the **Enabled** check box to enable the event rule, or uncheck the box to disable the rule.
4. Click **OK**.

Editing event rules

To edit a response rule:

1. Click **Tools→Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab.
3. Select the rule you want to edit, and click the **Edit** icon.
4. Edit the rule as necessary.
5. Click **OK**.

Removing event rules

To remove an event rule:

1. Click **Tools→Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab.
3. Select the rule you want to edit, and click the **Delete** icon.

Ordering event rules

To change the order of response rules:

1. Click **Tools→Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab.
3. Select a rule in the list, and then click the **Move Up** or **Move Down** options on the toolbar to change the order of the rule in the list.
4. Click **Apply**.

Customizing the Event Rules Tab

Introduction

You can customize how rules appear on the Event Rules tab to help you find important information when you need it. This topic describes the following tasks:

- adding and removing columns on the Event Rules tab
- sorting information in a column
- grouping rules by column

Adding or removing columns

To add or remove columns on the Event Rules tab:

1. Click **Tools→Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab, and then click **Select Columns**.
3. Select the check box beside the column you want to add or remove from the view.
4. Click **OK**, and then click **OK** on the Central Responses window.

Sorting information in a column

To sort information in a column:

1. Click **Tools→Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab.
3. Click the column header for the column you want to sort.

   The information is sorted alphabetically or numerically within the column.
4. Click **OK**.

Grouping rules by column

To group rules by column:

1. Click **Tools→Central Responses**, and then click **Response Rules**.
2. Select the **Event Rules** tab, and then click **Group By**.
3. In the **All Columns** list, select the column you want to use to group information.
4. Click **Add**.

   The column name appears in the Group by These Columns List.

   Tip: You can also right-click any column heading, and then click **Group by** on the pop-up menu to group rules by column.

   Each column you add to the list is nested under the previous column. To change how columns are nested, you must remove them from the list, and then add them back to the list in the desired order.
5. Click **OK**.

Chapter 9

Defining Component Rules

Overview

Introduction

This chapter provides information about defining component rules, which are Response Rules based on status changes in SiteProtector components and agents.

In this section

This chapter contains the following topics:

Topic	Page
What is a Component Rule?	72
Creating Component Rules	73

What is a Component Rule?

Introduction

This topic provides introductory information about component rules.

Definition

Component rules are user-defined parameters that cause SiteProtector to send a response when the status of an agent or component changes.

Examples: The following are examples of component rules:

- the agent status that must reported
- the amount of time the agent status must be reported

Restriction

You can create up to 100 component rules. Using more than 100 component rules can cause negative performance issues with your system.

Creating Component Rules

Introduction

When you create component rules, as the status or state of a component changes, it is matched to the component rules that you have created. If a status on a component matches a rule's criteria, then SiteProtector determines if all the other parameters match as well. If all parameters match the rule, SiteProtector generates a response.

Task overview

Table 10 describes the tasks required to create a component rule:

Task	Description
1	Set up rule details such as name.
2	Specify filters for the rule.
3	Specify the component address for the rule.
4	Specify the response for the rule.
5	Specify advanced filters for the rule.

Table 10: *Tasks for creating a component rule*

Setting up rule details

To create a component rule:

1. Click **Tools→Central Responses**, and then click **Response Rules**.
2. Select the **Component Rules** tab, and then click **Add**.
3. Select the **Enabled** check box, and then define the following rule details:

Field	Description
Order	This value is system-defined based on the rules location in the rule list.
Name	Type a name for the rule. The text box allows 50 characters.
Comment	Type user-defined comments about the rule. The text box allows 255 characters.

4. Go to next procedure to specify rule filters.

Specifying rule filters

To specify the filters for the rule:

1. Select the **Filters** tab.
2. In the **Status** section, select the component statuses that you want to trigger the rule.
3. In the **Type** section, select the types of components that must have the statuses you selected to trigger the rule.
4. Go to the next procedure in this topic to specify component addresses.

Specifying component addresses

To specify component addresses:

1. Select the **Component Address** tab.
2. In the **Component Address** section, select one of the following options, and then provide the information as described:

Option	Description
Any	No input required.
Single IP Address	Do one of the following: • Select an IP address from the list. • Click **Add**, and then type the IP address such as 128.8.27.18.
Network Address / #Network Bits (CIDR)	Type the **IP address** and **subnet mask** such as 128.8.27.18 / 16. The *mask* is the network identifier. This is a number from 1 to 32.
IP Address Range	Type the beginning and ending IP address for the range such as 128.8.27.18 - 128.8.27.28.
Address List Entry	Do one of the following: • Select a name from the **Address List Entry Name** list. • Click **Add Address Name**, and then create the name.

3. Go to the next procedure in this topic to specify a response for the rule.

Specifying E-mail Responses

To specify e-mail responses:

1. On the Responses tab, select the **Response Frequency** check box, and then type or select the appropriate values for **Send at most** ***[n]*** **responses within** ***[n] [time period]***.

   Note: The default is 1 response within 60 seconds. If you do not specify a response frequency, then SiteProtector sends a notification every time the rule is matched.

2. Complete one or more of the following tasks:

   Note: You create the e-mail, SNMP, or user-specified responses that appear in **Response Rules** on the **Responses** tab. If you do not see the e-mail, SNMP, or user-specified information you want to associate with this rule in the list, click **Manage Responses** to add it to the list.

   - Select the **E-mail** tab, and then select the check box in the **Enabled** column for the e-mail response to associate with this rule.
   - Select the **SNMP** tab, and then select the check box in the **Enabled** column for the SNMP response to associate with this rule.
   - Select the **User-Specified** tab, and then follow the instructions for "Configuring User-Specified Response Objects" on page 47.

3. Select another tab to continue, or click **OK**.

Specifying SNMP Responses

To specify a SNMP response:

1. Select the **Responses** tab.
2. Specify the response frequency.
3. Select the **SNMP** tab.

4. Does the rule exist in the list?
   - If *yes*, select the rule, and then go to the next procedure in this topic to specify advanced filters.
   - If *no*, go to Step 5.
5. Click **Add**.

   The Add SNMP dialog box appears.
6. Type a **Name** to associate with the SNMP response.
7. Type the IP address to which the trap is sent in the **Manager** box.
8. Type the valid **Community name** the system uses to authenticate with the SNMP agent.
9. Click **OK**, and then go to the next procedure to specify advanced filters for the rule.

Specifying User Specified Responses

To specify a user specified response:

1. Select the **Responses** tab.
2. Specify the response frequency.
3. Select the **User Specified** tab.
4. Does the rule exist in the list?
   - If *yes*, select the rule, and then go to the next procedure in this topic to specify advanced filters.
   - If *no*, go to Step 5.
5. Click **Add**.
6. Type a descriptive **Name** for the object.
7. Type a **Command** to associate with the object.
8. Expand the **Common Parameters** folder, and then select a parameter.
9. Click **Add**.
10. Click **Move Up** or **Move Down** to order the parameters you have added to the list.
11. Click **OK**, and then go to the next procedure to specify advanced filters.

Specifying advanced filters for component rules

To specify advanced filters:

1. Select the Advanced Filters tab.
2. Does the advanced filter exist in the list?
   - If *yes*, select the filter, and then click **OK** to complete the process for creating a component rule.
   - If *no*, go to Step 3.
3. Click **Add**.

   After you click **Add**, you have three choices: ComponentName, ComponentHostName, and ComponentVersion. You cannot add custom parameters.

Chapter 10

Defining Network Objects

Overview

Introduction

This chapter provides information about defining Network Objects.

You should define Network Objects before you configure policies for agents that you want to use them.

In this chapter

This chapter contains the following topics:

Topic	Page
What are Network Objects?	78
Defining Address Names in Network Objects	80
Defining Address Groups in Network Objects	82
Defining Port Names in Network Objects	84
Defining Port Groups in Network Objects	86
Defining Dynamic Address Names in Network Objects	88
Exporting and Importing Network Objects Data	90

What are Network Objects?

Introduction

Network Objects store frequently used IP addresses, ports, and other information in a single, reusable object. Network Objects provide a central location for managing this information. If a Network Object is used by three agents, then you only have to update the information once, and the information will be updated for all three agents simultaneously.

Note: Network Objects reside in the Shared Objects node of the Policy repository. Central Responses can only use Network Objects that reside in the default repository.
For more information on Shared Objects, See "Shared Objects" on page 20.

Information in Network Objects

Network Objects can include the following information:

- address names
- address groups (for Proventia Network MFS responses only)
- port names
- port groups (for Proventia Network MFS responses only)
- dynamic address list (for Proventia Network MFS responses only)

Advantages

Network Objects provide the following advantages:

- They capture a complex set of frequently used information, such as IP addresses, in a single, reusable object. The policy can be used at any time during policy and response configuration.
- They eliminate the need to re-enter large amounts of information each time you create a security policy and response.
- They provide an efficient method for updating information, such as IP addresses and ports, used in policies and responses. You change the information once, and the changes are reflected anywhere the Network Object is used.

Simple and complex objects

Network Objects can be simple or complex depending on your requirements. The most simple object contains a single IP address or port. For example, if you often use the IP address 127.0.0.1, then you can define the object to include the single IP address 127.0.0.1. More complex network objects contain a combination of information, such as a range of IP addresses and a range of ports. For example, you create a Network Object called *Boston Web Servers* that includes all of the following information:

- IP address range of 192.0.2.0 - 192.0.2.24
- Port range of 100 - 300

Task overview

Table 11 describes the tasks for defining a Network Objects policy:

Task	Description
1	Define address names in the policy. See "Defining Address Names in Network Objects" on page 80.

Table 11: *Tasks for defining a Network Objects policy*

Task	Description
2	Define address groups in the policy. See “Defining Address Groups in Network Objects” on page 82.
3	Define ports in the policy. See “Defining Port Names in Network Objects” on page 84.
4	Define port groups in the policy. See “Defining Port Groups in Network Objects” on page 86.
5	Define dynamic address names in the policy. See “Defining Dynamic Address Names in Network Objects” on page 88.

Table 11: *Tasks for defining a Network Objects policy (Continued)*

Defining Address Names in Network Objects

Introduction

This topic provides information about adding, editing, and removing address names in Network Objects.

When you edit or remove an address name and the address name is associated with response rule, you clear the association between the address name and the response rule. To restore the association, you must do one of the following:

- manually associate the response rule with the edited address name
- create a new association between the response rule and another address name

Description

An *address name* represents the following information:

- any IP address
- a single IP address
- a single IP address range
- a single IP address and CIDR mask
- a single address list
- a combination of any of this information

Adding address names

To add an address name to a Network Object:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Address Names** tab, and then click the **Add** icon.

   The Add Address Names window appears.
3. In the **Name** text box, type a name for the address name.

   Note: Do not include spaces in the name.
4. In the **Comment** text box, type a description of the address name.
5. In the **Address** section, select one of the following:

Option	Action
Single IP Address	Select this option to include a single IP address in the address name, and then do one of the following: • select the IP address in the list; this list includes addresses you defined in the Network Objects policy • click **Add**, and then add an address to the list
Network Address / #Network Bits (CIDR)	Select this option to include IP address and network mask in the address name, and then type the required information.
IP Address Range	Select this option to include an IP address range in the address name, and then type the IP address range.

Option	Action
IP Address List	Select this option to include a list of IP addresses in the address name, and then do one of the following: • type the **Address Entry List Name**; the name must be typed exactly as it appears in the Network Object policy • click **Add Address Names**, and then add a name to the Network Object policy.

6. In the Source Port section, select one of the following:
   - **Any**
   - **Single Por**t
   - **Port Range**
   - **Port List Entry**
7. Click **OK**, and then click **Apply**.

Editing address names

To edit an address name:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Address Names** tab.
3. Select the address name, and then click the **Edit** icon.
   The Edit Address Names window appears.
4. Change the address name as necessary, and then click **OK**.
5. Click **Apply**.

Removing address names

To remove an address name:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Address Names** tab.
3. Select the address name you want to remove, and then click the **Delete** icon.
4. Click **Yes** to in the alert window to confirm your changes.

Defining Address Groups in Network Objects

Introduction

This topic provides information about adding, removing, and editing address groups in Network Objects.

Description

An *address group* represents the following information:

- a single address name network object
- multiple address name network objects
- other address groups

Note: The Proventia Network MFS is the only agent that uses address groups.

Adding address groups

To add an address group to a Network Object:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Address Groups** tab, and then click the **Add** icon.

   The Add Address Names window appears.
3. Type a name and description for the address group.
4. Click **Add**.

   The Add Address window appears.
5. Select one of the following:

Option	Action
Address Name	Select this option to include an address name in the address group, and then select the name from the list. **Note:** You can use the **Address Names** button to add, edit, and remove address names in the list.
Dynamic Address	Select this option to include a dynamic address in the address group, and then select the name in the list. **Note:** You can use the **Dynamic Names** button to add, edit, and remove address names in the list.
Address Group	Select this option to include an address group in the address group, and then select the name in the list. **Note:** You can use the **Address Groups** button to add, edit, and remove address names in the list.

6. Click **OK**, and then click **Apply**.

Editing address groups

To edit an address group:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Address Groups** tab.
3. Select the address group, and then click the **Edit** icon.

   The Edit Address Names window appears.
4. Change the address group as necessary, and then click **OK**.

5. Click **Apply**.

Removing address groups

To remove an address group:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Address Groups** tab.
3. Select the address group, and then click the **Delete** icon.
4. Click **Yes** in the alert window to confirm you changes.

Defining Port Names in Network Objects

Information

This topic provides information about adding, removing, and editing port names in Network Objects.

Description

A *port name* represents the following information:

- a single port
- multiple ports
- a single port range
- multiple port ranges

The following agents use port names in Network Objects:

- Event Archiver
- Central Responses
- Proventia Network MFS responses

Adding port names

To add a port name to a Network Object:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Port Names** tab.

   Note: The Port Names tab provides lists of commonly used ports.
3. Do one of the following:
   - Select a port in the list, and then go to Step 8.
   - Click the Add icon to add a port, and then go to Step 5.
4. Type a name and comment for the port name.

   Note: Do not include spaces in the name.
5. Select one of the following protocols from the **Protocol** list:

Protocol	Description
TCP (Transmission Control Protocol)	Select this protocol if the port you are adding is used to exchange streams of data between hosts.
UDP (User Datagram Protocol)	Select this protocol if the port you are adding is used to send and receive data grams over a connection-less IP network. This protocol is also used for Unix trace route commands.

   Note: The Protocol is required.
6. In the **Address** section, select one of the following:
   - Select **Single Port**, and then type a port number.
   - Select **Port Range**, and then select a port range from the Range list.

   Note: You can use the icons to Add, Edit, and Remove entries on the Port Range list.
7. Click **OK**, and then click **Apply**.

Editing port names

To edit a port name:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Port Names** tab.
3. Select the port name, and then click the Edit icon.
4. Change the port name as necessary, and then click **OK**.
5. Click **Save All**.

Removing port names

To remove a port name:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Port Names** tab.
3. Select the port name, and then click the **Delete** icon.
4. Click **Yes** in the alert window to confirm your changes.

Defining Port Groups in Network Objects

Introduction

This topic provides information about adding, removing, and editing port groups in Network Objects. The Proventia Network MFS is the only agent that uses port groups in Network Objects.

When you edit or remove a port group and the port group is associated with a response rule, you clear the association between the address name and the response rule. To restore the association, you must do one of the following:

- manually associate the response rule with the edited address name
- create a new association between the response rule and another address name

Description

A *port group* represents the following information:

- a single port name
- multiple port names
- a single port group
- multiple port groups
- any combination of this information

Adding port groups

To add a port group:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Port Groups** tab.
3. In the right pane, select the **Port Groups** tab, and then click the **Add** icon.

   The Add Port Groups window appears.
4. Type a name and comment for the port group.
5. In the **Ports** section, click **Add**.
6. Select one of the following:

Option	Action
Port Name	Select this option to include a port name in the port group, and then select the name from the list. **Note:** You can use the **Port Names** button to add, edit, and remove address names in the list.
Port Group	Select this option to include a port group in the port group, and then select the name in the list.

7. Click **OK**, and then click **Apply**.

Editing port groups

To edit a port group:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Port Groups** tab.
3. Select the port group, and then click the Edit icon.
4. Change the port group as necessary, and then click **OK**.
5. Click **Apply**.

Removing port groups

To remove a port group:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Port Groups** tab.
3. Select the port group, and then click the **Delete** icon.
4. Click **Yes** in the alert window to confirm your changes.

Defining Dynamic Address Names in Network Objects

Introduction

This topic provides information about adding, removing, and editing dynamic address names in Network Objects.

Description: dynamic address name

A *dynamic address name* represents multiple dynamic address lists from different Proventia Network MFS. Before the dynamic address name can represent the multiple lists, you must associate the dynamic address name with the different dynamic address lists. You perform this task with the Proventia Network MFS interface, not in SiteProtector.

Description: dynamic address list

A *dynamic address list* represents addresses specific to Proventia Network MFS. The Proventia Network MFS-specific addresses are associated with a dynamic address name. A dynamic address list appears only when you access the policy editor with the Proventia Manager.

Default dynamic address names

Table 12 describes the default dynamic address names included in the Network Objects policy:

Name	Description
CORP	The CORP dynamic address name automatically stores the IP address and subnet mask for the Proventia Network MFS internal interface. When you upgrade the Proventia Network MFS firmware, the upgrade process migrates this information to the new system. For new Proventia Network MFS, you must enter this information during the appliance setup process.
DMZ	The DMZ dynamic address name does not automatically store any information about the Proventia Network MFS. When you upgrade the Proventia Network MFS firmware, the upgrade process automatically migrates this information to the new system. For new Proventia Network MFS, you must enter this information during the appliance setup process.

Table 12: *Default dynamic address name descriptions*

Tasks overview

Table 13 describes the tasks for creating a single dynamic address name that represents multiple dynamic address lists:

Task	Description
1	Add a dynamic address name.
2	Add a dynamic address list that includes the IP addresses for each Proventia Network MFS appliance.
3	For each Proventia Network MFS appliance, associate the IP address for the appliance with the dynamic address list.

Table 13: *Tasks for associating dynamic address names with dynamic address lists*

Adding dynamic address names

To add a dynamic address name to a Network Object:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Dynamic Address Names** tab, and then click the Add icon.
   The Add Dynamic Address Names window appears.
3. Type a name and comment for the dynamic address name.
   Important: Do not include spaces in the name.
4. Click **OK**, and then click **Apply**.

Editing dynamic address names

To edit dynamic address names:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Dynamic Address Names** tab.
3. Select the name, and then click the **Edit** icon.
4. Change the information as necessary, and then click **OK**.
5. Click **Apply**.

Removing dynamic address names

To remove dynamic address names:

1. Click **Tools→Central Responses**, and then click **Network Objects**.
2. Select the **Dynamic Address Names** tab.
3. Select the name, and then click the **Delete** icon.
4. Click **Yes** in the alert window to confirm your changes.

Exporting and Importing Network Objects Data

Introduction

This topic provides information about exporting and importing data to and from Network Objects, such as address names and port names.

Exporting data from the Network Objects policy

To export data from a Network Object:

1. Select **Policy** from the **Go To** list.
2. Expand the repository and Shared Objects nodes, and then select **Network Objects**.
3. Click **Object→ Open**, and then select the tab for the type of information you want to export.
4. Select the data you want to export, and then click **Action→ Export**.
5. Type a **Name** for the network object.
6. Navigate to the location where you want to save the object.
7. Click **Save**.

   The network object is saved to the user-specified location.

Importing data into the Network Objects policy

To import data into a Network Object:

1. Select **Policy** from the **Go to** list.
2. Expand the repository and Shared Objects nodes, and then select **Network Objects**.
3. Click **Object→ Open**.
4. Select the tab for the type of information you want to export, and then click **Action→ Import**.
5. Navigate to the file you want to import, and then click **Open**.
6. The item is imported into the Network Object.
7. Click **Action→ Save Policy**.

Part III

Configuring Site-Level Policies and Responses

Chapter 11

Configuring Site-Level Policies

Overview

Introduction

This chapter provides information about how to configure and apply policies for the following:

- RealSecure Desktop 7.0
- Proventia Desktop 8.0
- Network Sensor 6.5 and 7.0
- Server Sensor 7.0
- Proventia G-series appliances

In this chapter

This chapter contains the following topics:

Topic	Page
What Are Policies?	94
Configuring Custom Policies	96
Applying Policies to Individual Agents	97
Applying Policies to Groups	98
Applying Policies with Policy Subscription Groups	100
Granting Users Permission to Modify Site-Level Policies	104
Policy Assignment with Active Directory	105

What Are Policies?

Introduction

Policies control the following agent behaviors:

- the type and volume of security events that an agent detects
- the priority of security events that the agent detects
- the agent's response to security events

Methods for applying policies

Table 14 describes the methods for applying policies to Network Sensors, Servers Sensors, and Proventia G appliances:

Method	Description
Apply the policy to an individual agent	You apply the policy directly to the individual agent. See "Applying Policies to Individual Agents" on page 97.
Apply the policy to a group	You apply the policy to the group that contains the agent. SiteProtector applies the policy to all agents contained in the group. **Note:** The Site Group, also called the top level group in the Site, is considered a group. You can apply policies to agents at the Site Group. See "Applying Policies to Groups" on page 98.
Apply the policy to a policy subscription group	You apply the policy to a group that is assigned to an agent to serve as the agent's policy subscription group. The agent gets its policy from the policy subscription group. See "Applying Policies with Policy Subscription Groups" on page 100.

Table 14: *Methods for applying policies to Network Sensors, Server Sensors, and Proventia G appliances*

How policies are applied to different agents

Table 15 describes how policies are applied to different agents:

Agent	Description
Network Sensor Server Sensor Proventia Network IPS	You can apply policies to these agents as follows: • Apply the policy directly to the individual agent. See "Applying Policies to Individual Agents" on page 97. • Apply the policy to a group of agents. See "Applying Policies to Groups" on page 98. • Apply the policy with a policy subscription group.
Desktop Protection agent	Desktop Protection agents *subscribe* to another group for their policies. This feature is called a *policy subscription group*. See "Applying Policies with Policy Subscription Groups" on page 100.
Network Internet Scanner	You apply policies to the Network Internet Scanner jobs each time you run the scan. You do *not* apply policies directly to the Network Internet Scanner or to a group of scanners.

Table 15: *How different agents get policies*

Site-level policy editor

For the following agents, you create and manage custom policies with the Site-level policy editor:

- RealSecure Desktop 7.0
- Network Sensor 6.5 and 7.0
- Server Sensor 7.0
- Proventia Network IPS

Note: The Site-level policy editor allows you to edit policies individually. You cannot, however, edit *multiple* policies using the Site-level policy editor.

Accessing the Site-level policy editor

You can access the Site-level policy editor at the Site Node level or at the individual agent level in the Console.

To access the Site-level policy editor:

- Select the Site Node, and then click **Action→Manage Policy**.

  Note: The Site Node appears as either of the following in the left pane:

  - `localhost`
  - IP address of the Application Server

Using the Site-level policy editor

Table 16 lists where you can find help for topics such as customizing, printing, and applying policies with the Site-level policy editor:

Product	Help for Policy Editor
Network Internet Scanner	Network Internet Scanner Policy Editor Help
Network Sensor	Response, Policy, and Event Collector Help
Proventia Network IPS	Response, Policy, and Event Collector Help
Proventia Desktop	Proventia Desktop Policy Editor Help
RealSecure Desktop 7.0	SiteProtector Help
SecurityFusion Module 2.0	SecurityFusion Module Policy Editor Help
Server Sensor 7.0	Response, Policy, and Event Collector Help

Table 16: *Help for Policy Editor for "Site-level policy" agents*

Configuring Custom Policies

Introduction

This topic provides instructions for configuring custom policies based on the predefined policies included with SiteProtector.

Important: You cannot make changes to a predefined policy.

Environments

SiteProtector provides predefined policies for the following environments:

- Windows
- Solaris
- Linux

Configuring custom policies

To configure a custom policy:

1. In the left pane, select the Site Node, and then click **Action→Manage Policy**.
   The Policy tab appears.
2. Select the policy, and then select **Action→Derive New**.
   The Derive New Item window appears.
3. Type the name for the custom policy, and then click **OK**.
   The Policy Editor appears.
4. Edit the policy in the Policy Editor.
   For more information about using the Policy Editor, refer to the Policy Editor help.
5. Save the policy.
   The policy is available for you to apply to "Site-level policy" agents.

Applying Policies to Individual Agents

Introduction

This topic explains how to apply policies to the following agents:

- Network Sensors
- Server Sensors
- Proventia Network IPS

Applying policies to agents

To apply a policy to an individual Network Sensor, Server Sensor, or Proventia Network IPS:

1. In the left pane, select the group that contains the agent.
2. Select **Agent** from the **Go to** list.
3. In the right pane, select the agent, and then click **Action→ Apply→ Policy**.

   The Apply Policy window appears. The Command Details section lists the Action (Apply Policy), the Asset where the agent is installed, and the Agent Type.
4. Click the **Policy** icon, and then select a policy from the list.
5. Click the **Schedule** icon, and then do one of the following:
   - select **Run Once** to apply the policy immediately
   - schedule a job to apply the policy
6. Click **OK**.

Applying Policies to Groups

Introduction

This topic provides information about applying policies to a group.

Reference: For information about how to apply policies to agents of the same type but in different groups, see "Applying Policies with Policy Subscription Groups" on page 100.

Assigning a policy to groups

In addition to applying policies to individual agents, you can apply policies to agents in the same group. SiteProtector provides the ability to perform the following policy assignment tasks at the group level:

- apply the same policy to multiple agents of the same type in the same group

  For example, apply a policy to all the network sensors in a group called Network Sensors.
- apply different policies to multiple agents of the same type in the same group

  For example, apply two different policies to the network sensors in a group called Network Sensors.
- apply different policies to different types of agents in the same group

  For example, apply a network sensor policy and a server sensor policy to a group that contains both agents.

Applying policies to groups provides an efficient method for managing and applying policies to multiple agents in the same group. This approach does not prevent you from also applying policies to the individual agents in the group. For example, you can apply a network sensor policy to a group that contains network sensors, and then apply an additional network sensor policy to an individual network sensor in the group.

Load distribution

When you apply a policy to a group of agents, SiteProtector does not apply the policy to all agents at the same time. It divides the agents into groups and applies the policy to the groups incrementally over a period of time.

Applying policies to agents in a group

To apply a policy to an agent in a group:

1. In the left pane, select the group that contains the agents, and then click **Action→ Apply→ Policy**.

   The Apply Policy window appears.
2. In the **Agent Type** list, select the type of agent that will receive the policy assignment:
   - Network Sensor
   - Proventia G-Series
   - Server Sensor
3. Click the **Policy** icon, and then select a policy from the list.
4. Do one of the following:
   - To apply the policy to only agents that subscribe to the group, select the **Only applies to subscribers** check box.
   - To apply the policy to all agents in the group, clear the check box.

5. Click the **Schedule** icon, and then do one of the following:
   - select **Run Once** to apply the policy immediately
   - schedule a job to apply the policy
6. Click **OK**.

Applying Policies with Policy Subscription Groups

Introduction

This topic provides information about policy subscription groups and how to apply policies to agents with policy subscription groups.

What is a policy subscription group?

A *policy subscription group* is like any other group in SiteProtector except that agents subscribe to the group for their policies. The policy subscription groups acts like a central distribution center for the policy. It provides an efficient method for managing policies for a large number of agents in a central location. It also eliminates the need to apply the policy to each individual agent.

For example, 10,000 Desktop Protection agents can subscribe to a single policy subscription group for their policies. You can manage and change the policy in the policy subscription group, and all 10,000 subscriber agents will be updated at the same time.

What indicates a policy subscription group?

Policy subscription groups appear in the left pane along with all other groups. There is no visual distinction between these types of groups and other groups in the Console. For this reason, you should give policy subscription groups a name to indicate the purpose of the group, such as Policy Group for Desktop Protection Agents. The procedure for creating a policy subscription group is the same procedure for creating a regular group.

Agents

You can configure the following agents to subscribe to a policy subscription group for their policies:

- Desktop Protection agents
- Network Sensors
- Server Sensors
- Proventia Network IPS

Example

The following example illustrates how you apply policies to agents with a policy subscription group:

- You create a group called "Policy Group for Desktop Protection Agents 8.0."
- You deploy 10,000 Desktop Protection agents on your network.
- You define a policy for the Desktop Protection agents, and then apply it to the Policy Group for Desktop Protection Agents 8.0 group.
- You assign the Policy Group for Desktop Protection Agents 8.0 group to all 10,000 Desktop Protection agents as their policy subscription group. All 10,000 agents get their policy from this one group.

  Note: For this feature to work, all of the agents must exist in subgroups below the Policy Group for Desktop Protection Agents 8.0 group. In other words, the Policy Group for Desktop Protection Agents 8.0 group must be the parent group with policy for all of the agents. Agents cannot get their policy from a subgroup, only a parent group or the group in which they exist.
- You change the policy and reapply it to the Policy Group for Desktop Protection Agents 8.0 group. All 10,000 subscriber agents are updated simultaneously.

Rules

When you apply policies with policy subscription groups, you must follow these rules:

- The policy subscription group must be a parent group to the groups that contain the subscriber groups. Agents cannot subscribe to a subgroup for their policies.
- An agent can subscribe to only one group for its policy. An agent cannot subscribe to multiple groups for different policies. If an agent subscribes to multiple groups, then the agent gets its policy from that last group it subscribed to.
- Agents of different versions must subscribe to different groups for their custom policies. For example, RealSecure Desktop 7.0 and Proventia Desktop 8.0 cannot subscribe to the same group for their policies. You must create two different groups, apply the different policies to the groups, and then set the different agents to subscribe to the appropriate group based on their version.
- Agents of different types can subscribe to the same group for their policies. For example, a network sensor and a server sensor can subscribe to the same group for their policies.
- You can apply only one policy to a policy subscription group for each agent type. For example, you cannot apply two different network sensor policies to the same policy subscription group.
- In addition to the single policy that you can apply to the policy subscription group for the Desktop Protection agent, you can also apply one policy for each of the following:
  - Network sensor
  - Server sensor
  - Network Intrusion Detection System and Proventia Network IPS

Task overview

Table 17 describes the tasks for applying a policy to agents with a policy subscription group:

Task	Description
1	Create a group, and then define the group settings. Give the group a name to indicates its purpose, such as “Policy Group for Desktop Protection Agents.” **Note:** You assign this group to the agent as the agent’s policy subscription group. The agent gets its policies from this group. The group must be a parent group to the group where the agent exists. See the *SiteProtector Configuration Guide*.
2	Create a custom policy for the agent. See “Configuring Custom Policies” on page 96.
3	Apply the custom policy to the group. **Note:** SiteProtector applies the policies to any agent that subscribes to the group. See “Applying Policies to Groups” on page 98.
4	Assign the group to the agent as the agent’s policy subscription group. **Note:** If you are applying the policy to a large number of agents, then you must assign the policy subscription group to all the agents.

Table 17: *Tasks for applying policies with policy subscription groups*

Assigning policy subscription groups to agents

To assign a policy subscription group to an agent:

1. Select the group that contains the agent.
2. Select **Agent** from the **Go to** list.

3. In the right pane, select the agent.
4. Click **Action→Configure Agents→Assign Policy Subscription Group**.
5. The Assign Policy Subscription Group window appears.
6. Verify the Agent Type.
7. In the Select Policy Group section, select a group, and then click **OK**.

   The agent subscribes to this group for its policies. If you move the agent from its current group, then the continues to get its policy from the policy subscription group.

Viewing policy subscription group settings

To view the policy subscription group setting for an agent:

1. Select the group that contains the agent.
2. Select **Agent** from the **Go to** list.
3. In the right pane, locate the **Get Policy From** column.

   This column indicates the group where the agent gets its policy from. This group is the agent's policy subscription group.

Assigning policy subscription groups

When you move an agent from the Ungrouped Assets folder into another group, SiteProtector attempts to set the agent's policy subscription group automatically. The success of this process depends on whether the group where you add the agent has a policy set correctly. Table 18 describes how SiteProtector sets the policy subscription group for agents that you manually add to other groups:

If you add the agent to a group that...	Then...
has a policy of the correct type set	SiteProtector sets this group to be the agent's policy subscription group.
does not have a policy of the correct type set	• SiteProtector searches the group hierarchy, moving up toward the top group, until it finds a group with the correct policy. • SiteProtector then sets first group it finds with a correct policy to be the agent's policy subscription group. If SiteProtector cannot find a group with the correct policy, then SiteProtector does not set the agent's policy subscription group.

Table 18: *How agents are assigned to a policy subscription group*

Working with Policies for Desktop Protection Agents

Introduction

This topic provides information about the following tasks:

- configuring custom policies for RealSecure Desktop 7.0
- applying policies to these agents

  Note: You apply the policy to a policy subscription group, and the Desktop Protection agents subscribe to this group for their policies. The **Get Policy From** column in the Console indicates the group that a Desktop Protection agent gets its policy from.

Important: You should assign Desktop Protection policies to a policy subscription group based on the level of security you want to provide the assets in the group.

Example

If you want to enforce different firewall rules for the Human Resources department and for the Finance department, then you should do the following:

- create a separate policy subscription group for each department
- assign different Desktop Protection policies to each group

Build requirements

Before you can generate an agent build, you must create a new Desktop Protection policy and assign it to the policy subscription group. SiteProtector provides several read-only Desktop Protection policies that you can use as a template to create the new policy, but you cannot use the read-only Desktop Protection policy to generate an agent builds. The read-only policies do not contain required information, such as the agent's software version or license string.

Procedure

To set policies for Desktop Protection agents:

1. Select the group that contains the Desktop Protection agents, and then select **Object→ Properties.**
2. In the Properties window, click **Details**.
3. In the right pane, right-click **RealSecure Desktop**, and then select **Set Policy**.

   The Select Policy window appears.
4. Is the policy you want to use in the list?
   - If *yes*, select the policy in the list, and then go to Step 9.
   - If *no*, go to Step 5.
5. Select a policy, and then click **Action→ Derive New**.

   The Derive New Item window appears.
6. Type a policy name in the **New item name** box, and then click **OK**.
7. Edit the policy as needed, and then click **Save**.

   The policy appears in the list.
8. Select the policy to apply to the group.
9. Click **OK**.

   The policy is applied to the group.

Granting Users Permission to Modify Site-Level Policies

Introduction

This topic explains how to grant a user permission to modify a policy in the Policy Editor. The Modify Policy permission is a Site-wide permission, meaning that the user can modify the policy anywhere in the Site.

Important: This procedure grants the user permission to modify an individual policy. The permission does not apply to all policies. If you want to grant a user the ability to modify multiple policies, then you must perform this procedure for each policy. SiteProtector does not provide a global permission that allows a user to modify all policies.

Procedure

To grant a user permission to modify a policy:

1. Select the Site Node, and then select **Action→Manage Policy**.

   The Policy tab appears.
2. Select the policy, and then click **Object→Properties** from the pop-up menu.

   The Details window for the policy appears.
3. Click **Permissions**.

   The Manage Permissions for *Policy Name* window appears.
4. In the **Users and/or Groups** section, click **Add** to add members or **Remove** to remove members.

   The list shows members who can modify the policy.
5. In the **Select Permission Action** section, select **Modify**

   This permission allows the user to modify this individual policy only.
6. Do you want to set or change the owner of the Site-level policy?
   - If *yes*, click **Advanced**, and then go to Step 7.
   - If *no*, click **OK** to finish.
7. In the **Change Owner** text box, type the member name for the owner, and then click **OK**.

   Note: You can also click **Check Names** to look up a member name.
8. Click **OK**, and then click **OK** again on the Details window.

   The user can now modify the individual response.

Policy Assignment with Active Directory

Introduction

If you use Active Directory to populate groups with assets in SiteProtector, then you may encounter issues related to policy assignments for agents. This topic describes some possible solutions for these issues.

Assets in multiple groups

When you put an asset in both an Active Directory group and a policy subscription group, and you can assign policies to both groups, the agent gets its policy based on the setting for the **Reassign agent policy based on Active Directory grouping** option. Table 19 describes the settings for this option:

Setting	Description
cleared	The agent continues to receive policies from the SiteProtector group.
selected	The agent receives its policy from the Active Directory group.

Table 19: *Policy assignment with an asset in multiple groups*

Moving an asset to a different Active Directory group in the same domain

Table 20 describes what happens if an agent subscribes to an Active Directory group for its policy, and the agent's asset is moved to a different Active Directory group on the network:

If the Active Directory information in SiteProtector is updated and the Reassign sensor policy check box is...	Then the agent...
cleared	continues to receive its policy from the original Active Directory group.
selected	receives its policy from the new Active Directory group.

Table 20: *Moving Active Directory assets within a domain*

Moving a computer object to a different domain in the same forest

If you move a computer object to a different domain in the same forest, what happens to the policy assigned to the original computer object depends on the Reassign sensor policy based on Active Directory grouping option, as shown in Table 21:

If the Reassign sensor policy based on Active Directory grouping check box is...	Then the policy...
cleared	remains assigned to the original computer object.
selected	assignment is unpredictable, and you should remove the computer object from the old domain to resolve the ambiguity.

Table 21: *Moving Active Directory assets to a different domain*

Moving an asset to a different domain in the same forest

Table 22 describes what happens if you move an asset to a different domain in the same forest, based on the method you use to move the asset:

If you…	Then…
join the computer to the new domain by renaming the domain in the computer's properties	• a new computer object is created in the new domain • the old computer object remains in the old domain • the new computer object receives a new GUID
use the Active Directory Migration Tool	• the old computer object remains in the old domain (in case you want to undo the operation) • the new computer object receives a new GUID
use the Microsoft MoveTree and Netdom utilities	• the old computer object is removed when the new computer object is created • the GUID does not change

Table 22: *Result of moving an asset to a different domain in the same forest*

Chapter 12

Configuring Site-Level Responses

Overview

Introduction

This chapter provides information about configuring agent responses and global responses for the following:

- Event Collector
- Network Sensor 6.5 and 7.0
- Server Sensor 6.5 and 7.0
- Proventia G-Series appliances

Important: This section does *not* apply to the following products:

- Network IPS
- Network IDS
- Network Multi-Function Security
- Proventia Server for Linux
- Proventia Server for Windows
- Proventia Desktop 8.0 or later
- Proventia Network ADS
- Proventia Network Mail Security

Reference

For step-by-step instructions about how to work with SiteProtector responses, see the *SiteProtector Help*.

In this chapter

This chapter contains the following topics:

Topic	Page
What Are Responses?	108
Configuring Custom Agent Responses	111
Granting Users Permission to Modify Site-Level Responses	112

What Are Responses?

Introduction

This topic provides information about responses.

Definition

A *response* is the action that an agent takes in response to a security event. For example, when an agent performs the following actions, the agent is *responding* to a security event:

- The agent notifies the Console to display information about the security event.
- The agent saves the security event to the Site Database.
- The agent sends an e-mail notification to a user regarding the security event.

These actions are user-defined and controlled through response settings.

Flexible responses

SiteProtector provides flexible response management and configuration options to meet your specific security and network requirements. For example, you can configure responses for the following:

- a single agent to send one response to the same individual security event
- a single agent to send multiple responses to the same individual security event
- multiple agents to send the same response to the same individual security event
- multiple agents to send different responses to the same individual security event

Required user input

When you configure responses, you must make decisions about how you want the agent to respond to the security event, such as the following:

- Do you want the agent to display the security event in the Console?
- Do you want the agent to save the security event to the Site Database?
- Do you want the agent to send an e-mail notification regarding the security event?
- What e-mail address should the agent send the e-mail to?
- How often do you want the agent to generate the response?

Your decisions determine how you should set the response options. You set some options in the response policy and other options outside of the response policy. Options set in the response policy are stored in the response file.

Global and agent responses

Table 23 describes the categories of responses:

Category	Description
Global	Global responses are Site-wide responses that control how all agents in the entire Site respond to security events. Global responses can be applied to the following agents: • Network Sensor • Server Sensor • Proventia Network IPS • SecurityFusion/Event Collector

Table 23: *Categories of responses*

Category	Description
Agent	Agent responses are Site-level responses that control how an individual agent responds to security events. Agent responses are also version specific, meaning that the response affects only agents at a specific version. Agent responses can be applied to the following agents: • Network Sensor • Server Sensor • Proventia Network IPS • SecurityFusion/Event Collector **Important:** Agent responses override global responses. For example, if you apply a global response and an agent response to an agent, then the agent responds based on the agent response, not the global response.

Table 23: *Categories of responses (Continued)*

Process

Follow this sequence when you configure responses:

1. Configure global responses.
2. Either merge the global responses with agent responses or entirely replace the agent responses with the global responses.

Supported responses by agent

Table 24 lists the supported response types for each agent:

Agent	Response Types
SecurityFusion/ Event Collector	These responses are available for the Event Collector through the SecurityFusion Module: • E-mail • SNMP • User-specified
Network Sensor	These responses are available for Network Sensor: • E-mail • Log Evidence • Opsec • RS-Kill • SNMP • User-specified
Network Sensor 6.5	These responses are available for Network Sensor: • E-mail • Opsec • Rskill • SNMP • User specified

Table 24: *Supported response types*

Agent	Response Types
Proventia Network IPS	These responses are available for Network Sensor: • E-mail • Opsec • Rskill • SNMP • User specified
Server Sensor 7.0	These responses are available for Network Sensor: • Banner • Block • E-mail • Fusion scripting • Rskill • SNMP • Suspend • User specified

Table 24: *Supported response types (Continued)*

Configuring Custom Agent Responses

Introduction

This topic provides information about configuring custom agent responses from the predefined responses.

Task overview

Table 25 describes the tasks for configuring responses to security events:

Task	Description
1	Configure a policy for the agent. In this task, you specify the *security events* that you want the agent to detect. This task requires the following procedures: • Select a policy. • Specify the events you want the agent to detect. • Save the policy. • Apply the policy to the agent. See “Configuring Site-Level Policies” on page 93.
2	Customize an agent response. In this task, you specify *responses*[a] that you want the agent to generate when it detects the security events.

Table 25: *Tasks for configuring responses*

a. SiteProtector provides a default response for each security event. A typical default response requires the agent to notify the Console of the security event and log the security event to the Site Database. The TCP reset, firewall reconfiguration, and user-defined response options are never selected in a default response.

Configuring custom agent responses

To configure a custom agent response:

1. Select the Site Node, and then select **Action→Manage Policy**.

   The Policy tab appears.

2. Click the **Response** icon.

   The right pane lists the responses.

3. Select the response, and then click **Action→Derive New**.

   The Derive New Item window appears.

4. Type the name for the custom response, and then click **OK**.

   The Response Editor appears.

5. Edit the response policy as necessary with the Response Policy Editor, and then click **OK**.

Granting Users Permission to Modify Site-Level Responses

Introduction

This topic explains how to grant a user permission to modify a response.

Important: This procedure grants the user permission to modify an *individual* response. The Modify Policy permission is a Site-wide permission, meaning that the user can modify the response anywhere in the Site. The permission does not apply to all responses. If you want to grant a user the ability to modify multiple responses, then you must perform this procedure for each response. SiteProtector does not provide a global permission that allows a user to modify all policies.

Procedure

To grant a user permission to modify a response:

1. Select the *Site Node*, and then click **Action→Manage Policy**.

   The Policy tab appears.
2. Click the **Response** icon.

   The right pane lists the responses.
3. Select the response, and then click **Object→Properties**.

   The Properties window appears.
4. Click **Permissions**.

   The Manage Permissions for *Response Policy Name* window appears.
5. In the **Users and/or Groups** section, click **Add** to add members or **Remove** to remove members.

   The list shows members who can create user-defined policies from this policy and view the policy.
6. In the **Select Permission Action** section, select **Modify**

   This permission allows the user to modify this individual policy only.
7. Do you want to set or change the owner of the response policy?
   - If *yes*, click **Advanced**, and then go to Step 8.
   - If *no*, click **OK** to finish.
8. In the **Change Owner** text box, type the member name for owner, and then click **OK**.

   You can also click **Check Names** to look up a member name.
9. Click **OK**, and then click **OK** again to close the Properties window.

   The user can now modify the individual response.