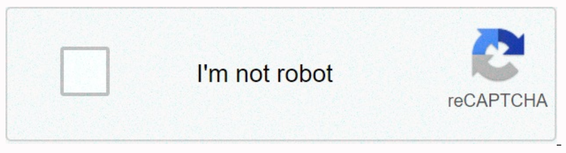

I'm not robot!

Trend micro imsva 9. 0 admin guide

highly scalable platform with centralized management, providing easyadministration. Optimized for high performance and continuous security, the applianceprovides comprehensive gateway email security. IMSVA Main Features and BenefitsThe following table outlines the main features and benefits that IMSVA can provide toyour network. TABLE 1-1. Main Features and Benefits FEATURE DESCRIPTIONS BENEFITS Data and system protection Cloud-basedpre-filtering ofmessages Cloud Pre-Filter integrates withIMSVA to scan all email trafficbefore it reaches your network. Cloud Pre-Filter can stopsignificant amounts of spam andmalicious messages (up to 90%of your total message traffic)from ever reaching your network. Emailencryption Trend Micro Email Encryptionintegrates with IMSVA to encrypt ordecrypt all email traffic entering andleaving your network. Trend Micro Email Encryptionprovides IMSVA the ability toencrypt all email messagesleaving your network. Byencrypting all email messagesleaving a network administratorscan prevent sensitive data frombeing leaked. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 1-4 FEATURE DESCRIPTIONS BENEFITS Advanced anti-malwareprotection The Advanced Threat Scan Engine(ATSE) uses a combination ofpattern-based scanning andaggressive heuristic scanning todetect document exploits and otherthreats used in targeted attacks. ATSE identifies both known andunknown advanced threats,protecting your system from newthreats that have yet to be addedto patterns. Command &Control (C&C)Contact AlertServices C&C Contact Alert Services allowsIMSVA to inspect the sender,recipients and reply-to addresses ina message's header, as well asURLs in the message body, to seeif any of them matches known C&Cobjects. C&C Contact Alert Servicesprovides IMSVA with enhanceddetection and alert capabilities tomitigate the damage caused byadvanced persistent threats andtargeted attacks. Graymail Graymail refers to solicited bulkemail messages that are not spam.IMSVA detects marketingmessages and newsletters andsocial network notifications asgraymail. IMSVA manages graymailseparately from common spamto allow administrators to identifygraymail messages. IPaddresses specified in thegraymail exception list bypassscanning. Regulatorycompliance Administrators can meetgovernment regulatoryrequirements using the new defaultpolicy scanning conditionsCompliance templates. Compliance templates provideadministrators with regulatorycompliance. For a detailed list ofavailable templates, see . //docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx //docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx Introducing InterScan Messaging Security Virtual Appliance 1-5 FEATURE DESCRIPTIONS BENEFITS Smart Scan Smart Scan facilitates a moreefficient scanning process by off-loading a large number of threatsignatures previously stored on theIMSVA server to the cloud. Smart Scan leverages the SmartProtection Network to: Enable fast, real-timesecurity status lookupcapabilities in the cloud Reduce the time necessaryto deliver protection againstemerging threats Lower memory consumptionon the server IntelliTrap Virus writers often attempt tocircumvent virus filtering by usingdifferent file compression schemes.IntelliTrap provides heuristicevaluation of these compressedfiles. Because there is the possibility thatIntelliTrap may identify a non-threatfile as a security risk, Trend Microrecommends quarantining messageattachments that fall into thiscategory when IntelliTrap isenabled. In addition, if your usersregularly exchange compressedfiles, you may want to disable thisfeature. By default, IntelliTrap is turned onas one of the scanning conditionsfor an antivirus policy, and isconfigured to quarantine messageattachments that may be classifiedas security risks. IntelliTrap helps reduce the riskthat a virus compressed usingdifferent file compressionschemes will enter your networkthrough email. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 1-6 FEATURE DESCRIPTIONS BENEFITS Contentmanagement IMSVA analyzes email messagesand their attachments, traveling toand from your network, forappropriate content. Content that you deeminappropriate, such as personalcommunication, largeattachments, and so on, can beblocked or deferred effectivelyusing IMSVA. Real-timeStatistics andMonitor Administrators can monitor thescan performance and IP filteringperformance of all IMSVA devices(within a group) on themanagement console. IMSVA provides administratorswith an overview of the systemthat keeps administratorsinformed on the first sign of mailprocessing issues. Detailedlogging helps administratorsproactively manage issuesbefore they become a problem. Protection against other email threats DoS attacks By flooding a mail server with largeattachments, or sending messagesthat contain multiple viruses orrecursively compressed files,individuals with malicious intent candisrupt mail processing. IMSVA allows you to configurethe characteristics of messagesthat you want to stop at theSMTP gateway, thus reducingthe chances of a DoS attack. Maliciousemail content Many types of file attachments,such as executable programs anddocuments with embedded macros,can harbor viruses. Messages withHTML script files, HTML links, Javaapplets, or ActiveX controls canalso perform harmful actions. IMSVA allows you to configurethe types of messages that areallowed to pass through theSMTP gateway. Introducing InterScan Messaging Security Virtual Appliance 1-7 FEATURE DESCRIPTIONS BENEFITS Degradation ofservices Non-business-related email traffichas become a problem in manyorganizations. Spam messagesconsume network bandwidth andaffect employee productivity. Someemployees use companymessaging systems to sendpersonal messages, transfer largemultimedia files, or conductpersonal business during workinghours. Most companies haveacceptable usage policies fortheir messaging systemIMSVAprovides tools to enforce andensure compliance with existingpolicies. Legal liabilityand businessintegrity Improper use of email can also puta company at risk of legal liability.Employees may engage in sexualor racial harassment, or other illegalactivity. Dishonest employees canuse a company messaging systemto leak confidential information.Inappropriate messages thatoriginate from a companys mailserver damage the companysreputation, even if the opinionsexpressed in the message are notthose of the company. IMSVA provides tools formonitoring and blocking contentto help reduce the risk thatmessages containinginappropriate or confidentialmaterial will be allowed throughyour gateway. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 1-8 FEATURE DESCRIPTIONS BENEFITS Mass mailingviruscontainment Email-borne viruses that mayautomatically spread bogusmessages through a companysmessaging system can beexpensive to clean up and causepanic among users. When IMSVA detects a mass-mailing virus, the action performedagainst this virus can be differentfrom the actions against other typesof viruses. For example, if IMSVA detects amacro virus in a Microsoft Officedocument with importantinformation, you can configure theprogram to quarantine the messageinstead of deleting the entiremessage, to ensure that importantinformation will not be lost.However, if IMSVA detects a mass-mailing virus, the program canautomatically delete the entiremessage. By auto-deleting messages thatcontain mass-mailing viruses,you avoid using server resourcesto scan, quarantine, or processmessages and files that have noredeeming value.

The identities of known mass-mailing viruses are in the MassMailing Pattern that is updatedusing the TrendLabsActiveUpdate Servers. You cansave resources, avoid help deskcalls from concerned employeesand eliminate post-outbreakcleanup work by choosing toautomatically delete these typesof viruses and their emailcontainers. Protection from spyware and other types of grayware Spyware andother types ofgrayware Other than viruses, your clients areat risk from potential threats suchas spyware, adware and dialers.For more information, see AboutSpyware/Grayware on page 1-14. IMSVAs ability to protect yourenvironment against spywareand other types of graywareenables you to significantlyreduce security, confidentiality,and legal risks to yourorganization. Integrated anti-spam features Introducing InterScan Messaging Security Virtual Appliance 1-9 FEATURE DESCRIPTIONS BENEFITS SpamPreventionSolution (SPS) Spam Prevention Solution (SPS) isa licensed product from TrendMicro that provides spam detectionservices to other Trend Microproducts.

To use SPS, obtain anSPS Activation Code. For moreinformation, contact your salesrepresentative. SPS works by using a built-in spamfilter that automatically becomesactive when you register andactivate the SPS license. The detection technology usedby Spam Prevention Solution(SPS) is based on sophisticatedcontent processing and statisticalanalysis. Unlike otherapproaches to identifying spam,content analysis provides high-performance, real-time detectionthat is highly adaptable, even asspam senders change theirtechniques. Spam Filteringwith IP Profilerand Emailreputation IP Profiler is a self-learning, fullyconfigurable feature that proactivelyblocks IP addresses of computersthat send spam and other types ofpotential threats. Email reputationblocks IP addresses of knownspam senders that Trend Micromaintains in a central database. NoteActivate SPS before youconfigure IP Profiler andEmail reputation. With the integration of IPFiltering, which includes IPProfiler and Email reputation,IMSVA can block spammers atthe IP level. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 1-10 FEATURE DESCRIPTIONS BENEFITS SocialEngineeringAttackProtection Social Engineering AttackProtection detects suspiciousbehavior related to socialengineering attacks in emailmessages. When Social Engineering AttackProtection is enabled, the TrendMicro Antispam Engine scans forsuspicious behavior in severalparts of each email transmission,including the email header,subject line, body, attachments,and the SMTP protocolinformation. If the AntispamEngine detects behaviorassociated with socialengineering attacks, theAntispam Engine returns detailsabout the message to IMSVA forfurther action, policyenforcement, or reporting. Administration and integration LDAP anddomain-basedpolicies You can configure LDAP settings ifyou are using LDAP directoryservices such as Lotus Dominoor Microsoft Active Directoryfor user-group definition andadministrator privileges. Using LDAP, you can definemultiple rules to enforce yourcompanys email usageguidelines.

You can define rulesfor individuals or groups, basedon the sender and recipientaddresses. Web-basedmanagementconsole The management console allowsyou to conveniently configureIMSVA policies and settings. The management console isSSL-compatible. Being SSL-compatible means access toIMSVA is more secure. Introducing InterScan Messaging Security Virtual Appliance 1-11 FEATURE DESCRIPTIONS BENEFITS End-UserQuarantine(EUQ) IMSVA provides web-based EUQ toimprove spam management. Theweb-based EUQ service allowsend-users to manage the spamquarantine of their personalaccounts and of distribution liststhat they belong to. IMSVAquarantines messages that itdetermines are spam. The EUQindexes these messages into adatabase. The messages are thenavailable for end-users to review,delete, or approve for delivery. With the web-based EUQmanagement console, end-userscan manage messages thatIMSVA quarantines. IMSVA also enables users toapply actions to quarantinedmessages and to add senders tothe Approved Senders listthrough links in the EUQ digest. Delegatedadministration IMSVA offers the ability to createdifferent access rights to themanagement console. You canchoose which sections of theconsole are accessible for differentadministrator logon accounts. By delegating administrativeroles to different employees, youcan promote the sharing ofadministrative duties. Centralizedreporting Centralized reporting gives you theflexibility of generating one time (ondemand) reports or scheduledreports. Helps you analyze how IMSVA isperforming. One time (on demand) reportsallow you to specify the type ofreport content as and whenrequired. Alternatively, you canconfigure IMSVA to automaticallygenerate reports daily, weekly,and monthly. Systemavailabilitymonitor A built-in agent monitors the healthof your IMSVA server and deliversnotifications through email orSNMP trap when a fault conditionthreatens to disrupt the mail flow. Email and SNMP notification ondetection of system failure allowsyou to take immediate correctiveactions and minimize downtime. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 1-12 FEATURE DESCRIPTIONS BENEFITS POP3scanning You can choose to enable ordisable POP3 scanning from themanagement console. In addition to SMTP traffic,IMSVA can also scan POP3messages at the gateway asmessaging clients in yournetwork retrieve them.

Clusteredarchitecture The current version of IMSVA hasbeen designed to make distributeddeployment possible.

You can install the variousIMSVA components on differentcomputers, and somecomponents can exist inmultiples. For example, if yourmessaging volume demands,you can install additional IMSVAscanner components onadditional servers, all using thesame policy services. Integrationwith VirtualAnalyzer IMSVA integrates with VirtualAnalyzer, which is an isolatedvirtual environment used to manageand analyze samples in DeepDiscovery Advisor and DeepDiscovery Analyzer. IMSVA sends suspiciousmessages, includingattachments, to Virtual Analyzerfor further analysis. VirtualAnalyzer performs contentsimulation and analysis in anisolated virtual environment toidentify characteristics commonlyassociated with many types ofmalware. In particular, VirtualAnalyzer checks if files attachedto messages contain exploitcode. Introducing InterScan Messaging Security Virtual Appliance 1-13 FEATURE DESCRIPTIONS BENEFITS Integrationwith TrendMicro ControlManager Trend Micro Control Manager(TMCM) is a software managementsolution that gives you the ability tocontrol antivirus and contentsecurity programs from a centrallocation regardless of the programsphysical location or platform. Thisapplication can simplify theadministration of a corporate virusand content security policy. Outbreak Prevention Servicesdelivered through Trend MicroControl Manager reduces therisk of outbreaks.

When a TrendMicro product detects a newemail-borne virus, TrendLabsissues a policy that uses theadvanced content filters inIMSVA to block messages byidentifying suspiciouscharacteristics in thesemessages. These rules helpminimize the window ofopportunity for an infectionbefore the updated pattern file isavailable. About Cloud Pre-FilterCloud Pre-Filter is a cloud security solution that integrates with IMSVA to provideproactive protection in the cloud with the privacy and control of an on-premise, virtualappliance. Cloud Pre-Filter reduces inbound email volume up to 90% by blocking spam andmalware outside your network. Cloud Pre-Filter is integrated with IMSVA at thegateway allowing flexible control over sensitive information. And local quarantinesensure your email stays private. No email is stored in the cloud. With Cloud Pre-Filter,you can reduce complexity and overhead to realize significant cost savings. About Email EncryptionTrend Micro Email Encryption provides IMSVA with the ability to perform encryptionand decryption of email. With Email Encryption, IMSVA has the ability to encrypt anddecrypt email regardless of the email client or platform from which it originated. Theencryption and decryption of email on Trend Micro Email Encryption is controlled by a Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 1-14 Policy Manager that enables an administrator to configure policies based on variousparameters, such as sender and recipient email addresses, keywords or where the email(or attachments) contain credit card numbers. Trend Micro Email Encryption presentsitself as a simple mail transfer protocol (SMTP) interface and delivers email out overSMTP to a configured outbound mail transport agent (MTA). This enables easyintegration with other email server-based products, be them content scanners, mailservers or archiving solutions. About Spyware/GraywareYour clients are at risk from potential threats other than viruses/malware. Grayware cannegatively affect the performance of the computers on your network and introducesignificant security, confidentiality, and legal risks to your organization. TABLE 1-2.

Types of Grayware TYPE DESCRIPTION Spyware Gathers data, such as account user names and passwords, andtransmits them to third parties Adware Displays advertisements and gathers data, such as user websurfing preferences, to target advertisements at the userthrough a web browser Dialers Changes computer Internet settings and can force a computerto dial pre-configured phone numbers through a modem Joke Programs Causes abnormal computer behavior, such as closing andopening the CD-ROM tray and displaying numerous messageboxes Hacking Tools Helps hackers enter computers Remote Access Tools Helps hackers remotely access and control computers Password CrackingApplications Helps hackers decipher account user names and passwords Other Other types not covered above Introducing InterScan Messaging Security Virtual Appliance 1-15 How Spyware/Grayware Gets into Your NetworkSpyware/grayware often gets into a corporate network when users download legitimatesoftware that has grayware applications included in the installation package. Most software programs include an End User License Agreement (EULA), which theuser has to accept before downloading. Often the EULA does include informationabout the application and its intended use to collect personal data; however, users oftenoverlook this information or do not understand the legal jargon. Potential Risks and ThreatsThe existence of spyware/grayware on your network has the potential to introduce thefollowing: TABLE 1-3. Types of Risks TYPE DESCRIPTION Reduced computerperformance To perform their tasks, spyware/grayware applications oftenrequire significant CPU and system memory resources. Increased webbrowser-relatedcrashes Certain types of grayware, such as adware, are often designedto create pop-up windows or display information in a browserframe or window. Depending on how the code in theseapplications interacts with system processes, grayware cansometimes cause browsers to crash or freeze and may evenrequire a system reboot. Reduced userefficiency By needing to close frequently occurring pop-up advertisementsand deal with the negative effects of joke programs, users canbe unnecessarily distracted from their main tasks. Degradation ofnetwork bandwidth Spyware/grayware applications often regularly transmit the datathey collect to other applications running on your network or tolocations outside of your network. Loss of personal andcorporate information Not all data that spyware/grayware applications collect is asinnocuous as a list of websites users visit. Spyware/graywarecan also collect the user names and passwords users type toaccess their personal accounts, such as a bank account, andcorporate accounts that access resources on your network. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 1-16 TYPE DESCRIPTION Higher risk of legalliability If hackers gain access to the computer resources on yournetwork, they may be able to utilize your client computers tolaunch attacks or install spyware/grayware on computersoutside your network. Having your network resources unwillinglyparticipate in these types of activities could leave yourorganization legally liable to damages incurred by other parties.

About Web Reputation ServicesTrend Micro web reputation technology helps break the infection chain by assigningwebsites a reputation based on an assessment of the trustworthiness of an URL,derived from an analysis of the domain. Web reputation protects against web-basedthreats including zero-day attacks, before they reach the network. Trend Micro webreputation technology tracks the lifecycle of hundreds of millions of web domains,extending proven Trend Micro anti-spam protection to the Internet. About Email ReputationTrend Micro designed Email reputation to identify and block spam before it enters acomputer network by routing Internet Protocol (IP) addresses of incoming mailconnections to Trend Micro Smart Protection Network for verification against anextensive Reputation Database. Types of Email ReputationThere are two types of Email reputation: Standard on page 1-16 and Advanced on page1-17. Email Reputation: Standard This service helps block spam by validating requested IP addresses against the TrendMicro reputation database, powered by the Trend Micro Smart Protection Network. Introducing InterScan Messaging Security Virtual Appliance 1-17 This ever-expanding database currently contains over 1 billion IP addresses withreputation ratings based on spamming activity. Trend Micro spam investigatorscontinuously review and update these ratings to ensure accuracy. Email reputation: Standard is a DNS single-query-based service.

Your designated emailserver makes a DNS query to the standard reputation database server whenever anincoming email message is received from an unknown host. If the host is listed in thestandard reputation database, Email reputation reports that email message as spam. Tip Trend Micro recommends that you configure IMSVA to block, not receive, any emailmessages from an IP address that is included on the standard reputation database. Email Reputation: Advanced Email reputation: Advanced identifies and stops sources of spam while they are in theprocess of sending millions of messages. This is a dynamic, real-time antispam solution. To provide this service, Trend Microcontinuously monitors network and traffic patterns and immediately updates thedynamic reputation database as new spam sources emerge, often within minutes of thefirst sign of spam. As evidence of spam activity ceases, the dynamic reputation databaseis updated accordingly. Like Email reputation: Standard, Email reputation: Advanced is a DNS query-basedservice, but two queries can be made to two different databases: the standard reputationdatabase and the dynamic reputation database (a database updated dynamically in realtime). These two databases have distinct entries (no overlapping IP addresses), allowingTrend Micro to maintain a very efficient and effective database that can quickly respondto highly dynamic sources of spam. Email reputation: Advanced has blocked more than80% of total incoming connections (all were malicious) in customer networks. Resultswill vary depending on how much of your incoming email stream is spam.

The morespam you receive, the higher the percentage of blocked connections you will see. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 1-18 About Trend Micro Control ManagerTrend Micro Control Manager is a software management solution that gives youthe ability to control antivirus and content security programs from a central location-regardless of the programs physical location or platform. This application can simplifythe administration of a corporate virus/malware and content security policy. Control Manager server: The Control Manager server is the machine upon whichthe Control Manager application is installed.

The web-based Control Managermanagement console is hosted from this server. Agent: The agent is an application installed on a managed product that allowsControl Manager to manage the product. The agent receives commands from theControl Manager server, and then applies them to the managed product. The agentcollects logs from the product, and sends them to Control Manager. Entity: An entity is a representation of a managed product on the ProductDirectory link. Each entity has an icon in the directory tree. The directory treedisplays all managed entities residing on the Control Manager console. Control Manager SupportThe following table shows a list of Control Manager features that IMSVA supports. TABLE 1-4. Supported Control Manager Features FEATURE DESCRIPTION SUPPORTED? Two-waycommunication Using 2-way communication,either IMSVA or ControlManager may initiate thecommunication process. No. Only IMSVA can initiate acommunication process withControl Manager. Introducing InterScan Messaging Security Virtual Appliance 1-19 FEATURE DESCRIPTION SUPPORTED? Outbreak PreventionPolicy The Outbreak PreventionPolicy (OPP) is a quickresponse to an outbreakdeveloped by TrendLabs thatcontains a list of actionsIMSVA should perform toreduce the likelihood of theIMSVA server or its clientsfrom becoming infected. Trend Micro ActiveUpdateServer deploys this policy toIMSVA through ControlManager. Yes Log upload for query Uploads IMSVA virus logs,Content Security logs, andEmail reputation logs toControl Manager for querypurposes. Yes Single Sign-on Manage IMSVA from ControlManager directly without firstlogging on to the IMSVAmanagement console. No. You need to first log on to theIMSVA management consolebefore you can manageIMSVA from Control Manager. Configurationreplication Replicate configurationsettings from an existingIMSVA server to a newIMSVA server from ControlManager. Yes Pattern update Update pattern files used byIMSVA from Control Manager Yes Engine update Update engines used byIMSVA from Control Manager. Yes Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 1-20 FEATURE DESCRIPTION SUPPORTED? Product componentupdate Update IMSVA productcomponents such as patchesand hot fixes from ControlManager. No. Refer to the specific patch orhot fix readme file forinstructions on how to updatethe product components. Configuration by userinterface redirect Configure IMSVA through theIMSVA management consoleaccessible from ControlManager. Yes Renew productregistration Renew IMSVA productlicense from Control Manager. Yes Customized reportingfrom Control Manager Control Manager providescustomized reporting and logqueries for email-related data. Yes Control Manager agentinstallation/uninstallation Install or uninstall IMSVAControl Manager agent fromControl Manager. No. IMSVA Control Manageragent is automaticallyinstalled when you installIMSVA. To enable/disable theagent, do the following fromthe IMSVA managementconsole: 1. Go to Administration >Connections. 2. Click the TMCM Servertab. 3. To enable/disable theagent, select/clear thecheck box next to EnableMCP Agent. Event notification Send IMSVA eventnotification from ControlManager. Yes Introducing InterScan Messaging Security Virtual Appliance 1-21 FEATURE DESCRIPTION SUPPORTED? Command tracking forall commands Track the status of commandsthat Control Manager issuesto IMSVA. Yes About Trend Micro Smart ProtectionTrend Micro provides next-generation content security through smart protectionservices. By processing threat information in the cloud, Trend Micro smart protectionreduces demand on system resources and eliminates time-consuming signaturedownloads. Smart protection services include: File Reputation ServicesFile reputation decouples the pattern file from the local scan engine andconducts pattern file lookups to the Trend Micro Smart Protection Network.High performance content delivery networks ensure minimum latency duringthe checking process and enable more immediate protection. Trend Micro continually enhances file reputation to improve malwaredetection. Smart Feedback allows Trend Micro to use community feedback offiles from millions of users to identify pertinent information that helpsdetermine the likelihood that a file is malicious. Web Reputation ServicesWith one of the largest reputation databases in the world, Trend Micro webreputation tracks the credibility of domains based on factors such as age,historical location changes, and suspicious activity indicators discoveredthrough malware behavior analysis. Trend Micro assigns reputation scores tospecific pages instead of classifying entire sites to increase accuracy and reducefalse positives. Web reputation technology prevents users from: Accessing compromised or infected sites Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 1-22 Communicating with Command & Control (C&C) servers used incybercrime The Need for a New SolutionThe conventional threat handling approach uses malware patterns or definitions that aredelivered to a client on a scheduled basis and stored locally.

To ensure continuedprotection, new updates need to be received and reloaded into the malware preventionsoftware regularly. While this method works, the continued increase in threat volume can impact server andworkstation performance, network bandwidth usage, and the overall time it takes todelivery quality protection. To address the exponential growth rate of threats, TrendMicro pioneered a smart approach that off-loads the storage of malware signatures tothe cloud. The technology and architecture used in this effort allows Trend Micro toprovide better protection to customers against the volume of emerging malware threats.

Trend Micro Smart Protection NetworkTrend Micro delivers File Reputation Services and Web Reputation Services to IMSVAthrough the Trend Micro Smart Protection Network. The Trend Micro Smart Protection Network is a next-generation cloud-client contentsecurity infrastructure designed to protect customers from security risks and webthreats. It powers both on-premise and Trend Micro hosted solutions to protect userswhether they are on the network, at home, or on the go. The Smart Protection Networkuses lighter-weight clients to access its unique in-the-cloud correlation of email, web,and file reputation technologies, as well as threat databases. Customers' protection isautomatically updated and strengthened as more products, services and users access thenetwork, creating a real-time neighborhood watch protection service for its users. The Smart Protection Network provides File Reputation Services by hosting themajority of the malware pattern definitions.

A client sends scan queries to the SmartProtection Network if its own pattern definitions cannot determine the risk of a file. The Smart Protection Network provides Web Reputation Services by hosting webreputation data previously available only through Trend Micro hosted servers. A clientsends web reputation queries to the Smart Protection Network to check the reputation Introducing InterScan Messaging Security Virtual Appliance 1-23 of websites that a user is attempting to access. The client correlates a website'sreputation with the specific web reputation policy enforced on the computer todetermine whether access to the site is allowed or blocked. For more information on the Smart Protection Network, visit: www.smartprotectionnetwork.com About Graymail ScanningGraymail refers to solicited bulk email messages that are not spam. IMSVA detectsmarketing messages and newsletters and social network notifications as graymail.IMSVA identifies graymail messages in two ways: Email Reputation Services scoring the source IP address Trend Micro Anti-Spam Engine identifying message content Note Note that while IMSVA detects these kinds of email messages, these messages are nottagged as spam.

Administrators define the rule criteria to take an action on those email messages. Everygraymail message rule has an exception list containing address objects that bypassmessage filtering. An address object is a single IP address or address range (IPv4 orIPv6), or the Classless Inter-Domain Routing (CIDR) block. Administrators have several options to understand graymail message traffic in thenetwork. Reports illustrate the highest senders and recipients of graymail messages fromexternal or internal sources. Administrators can also query detailed log information orview the email quarantine and release messages identified as permitted graymailmessages when necessary. The graymail exception list can be exported and imported. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 1-24 Note Ensure that IMSVA can query external DNS servers for graymail scanning.

If you changeany DNS server settings, restart the scanner server to load the new settings. About Command & Control (C&C) ContactAlert Services Trend Micro Command & Control (C&C) Contact Alert Services provides IMSVA withenhanced detection and alert capabilities to mitigate the damage caused by advancedpersistent threats and targeted attacks.

It leverages the Global Intelligence list compiled,tested, and rated by the Trend Micro Smart Protection Network to detect callbackaddresses. With C&C Contact Alert Services, IMSVA has the ability to inspect the sender,recipients and reply-to addresses in a message's header, as well as URLs in the messagebody, to see if any of them matches known C&C objects. Administrators can configureIMSVA to quarantine such messages and send a notification when a message is flagged.IMSVA logs all detected email with C&C objects and the action taken on thesemessages. IMSVA sends these logs to Control Manager for query purposes. 2-1 Chapter 2 Getting StartedThis chapter explains how to log on to the management console and providesinstructions on what to do immediately after installation to get IMSVA up and running. Topics include: Opening the IMSVA Management Console on page 2-2 Viewing the Management Console Using Secure Socket Layer on page 2-3 Setting Up a Child Device on page 2-4 Using Smart Search on page 2-6 Configuring Proxy Settings on page 2-6 IMSVA Services on page 2-8 Selecting a Scan Method on page 2-8 Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 2-2 Opening the IMSVA Management ConsoleYou can view the IMSVA management console using a web browser from the serverwhere you installed the program, or remotely across the network. Procedure 1. Type the following URL: https://:8445 Tip An alternative to using the IP address is to use the target servers fully qualifieddomain name (FQDN). 2. Type the logon credentials to open the management console. The default logon credentials are as follows: Administrator user name: admin Password: imsva 3. Click Log On. Note If you are using Internet Explorer to access the management console, InternetExplorer will block the access and display a popup dialog box indicating that thecertificate was issued from a different web address. Add the management console IPaddress to your Trusted sites list (Internet Options > Security in Internet Explorer)or ignore the message and click Continue to this website to proceed. When you log on for the first time, the Configuration Wizard screen appears. For detailed configurations in the Configuration Wizard, see Using theConfiguration Wizard on page 4-1. Getting Started 2-3 What to do next Trend Micro recommends changing the password regularly, to prevent unauthorizedaccess to the management console. Using the Online Help The IMSVA management console comes with an Online Help that provides adescription of each field on the user interface. To access page-specific Online Help from the IMSVA management console, click theHelp ( ) icon located at the top right corner of the page.

To access the table of contents for the Online Help, click the Help ( ) icon next tothe Log Off hyperlink on the right of the page header. FIGURE 2-1. Table of Contents Access for Online Help Viewing the Management Console UsingSecure Socket Layer The IMSVA management console supports encrypted communication, using SecureSocket Layer (SSL). After installing IMSVA, SSL communication should work becausethe installation contains a default certificate. Trend Micro suggests that you use yourown certificate to increase security. To use your own certificate, assign the certificate to the management console. Fordetails, see Assigning a Certificate on page 13-21. To create a certificate, see Creating a Self-Signed Certificate on page 13-14. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 2-4 Setting Up a Child DeviceThis section explains how to set up a child device and register it to the parent device.

Tip Trend Micro recommends using an NTP server if you intend to set up child devices. Doingso ensures that the time and date of devices in the IMSVA group are synchronized. Formore information, see Configuring NTP Settings on page 30-15. Procedure 1. Determine the Internal Communication Port IP address of the child device.

WARNING! Parent and child devices must use their Internal Communication Port tocommunicate with each other. If your parent device or your child devices havemultiple network interface cards (NIC), add a host-route entry by Command LineInterface (CLI) following the instructions below.

On the parent device in the CLI: configure network route add /32 On the child device in the CLI: configure network route add /32 2. After you set up a parent device, do the following: a. Make sure the parent device is operational. b.

Log on to the management console. Make sure that you are logging on to theparent device management console. c. Go to Administration > IMSVA Configuration > Connections > Child IP. Getting Started 2-5 d. Under Add IP Address, add the IP address for the Internal CommunicationPort of the child device. 3. On the child device, do the following: a.

Log on to the management console of the child device. All IMSVA deviceshave the same management console logon credentials. b. In the Setup Wizard, configure the local system settings and then click Next>.

c. On the Deployment Settings screen, select Child Server and add the IPaddress for the Internal Communication Port of the parent device. d. Click Finish. 4. On the parent device, do the following: a.

Go to System Status. b. Verify that the child device appears under Managed Services and that a greencheck mark ( ) appears under Connection. You can start or stop Scanner,Policy, or EUQ services. Note If you enabled EUQ on the parent, it will also be enabled on the child. 5. If you want to use EUQ on the child device, redistribute the data across the EUQdatabases: a. On the parent device, navigate to Administration > End-User Quarantine.

b. Select Redistribute all or Only redistribute to approved senders. Tip Trend Micro recommends choosing Redistribute all. c. Click Redistribute.

Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 2-6 Note If you registered an EUQ-enabled child device to its parent device, add sendersto the approved senders list, and then re-distribute EUQ data. Some of thenewly added approved senders might not appear. Trend Micro recommends the following: After redistributing EUQ, the administrator informs all end users to verifythat the newly added approved senders are still available. That the administrator notifies all end users not to add EUQ approvedsenders list when the administrator is adding a child device andredistributing EUQ. Using Smart SearchSmart Search provides a quick way to navigate to screens on the management console.Specify the name of the screen or the name of a feature in the Smart Search text boxand then select an entry from the drop-down list that appears. Configuring Proxy SettingsIf your network uses a proxy server, configure IMSVA proxy settings. Proxy settingsaffect the following: Component updates (pattern files and scan engines) Product license registration Web Reputation queries Cloud Pre-Filter service and Smart Feedback Trend Micro Email Encryption Certificate validation check Getting Started 2-7 Procedure 1. Go to Administration > Proxy. The Proxy screen appears.

2. Select Use a proxy server for updates to patterns, engines, licenses, WebReputation queries, Cloud Pre-Filter, and Trend Micro Email Encryption, and forcertificate validation check. 3. Specify the proxy protocol: HTTP, SOCKS4, or SOCKS5.

Tip When using Cloud Pre-Filter, Trend Micro recommends using HTTP or SOCKS5. Certificate validation check only uses HTTP. 4. Specify the host name or IP address of the proxy server. 5. Specify the port the proxy server uses to connect to the Internet. 6.

Specify the user name you need for administrative access to the proxy server. 7. Specify the corresponding password. 8. Click Save. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 2-8 IMSVA ServicesThe scanner and policy services must be started to start protecting your network usingIMSVA. You can, however, choose whether to install or start the EUQ service. Scanner Service: Performs scanning of SMTP/POP3 traffic. Policy Service: Acts as a remote store of rules for the scanner service to enhancerule lookups. EUQ Service: Hosts a web-based management console to enable end users to view,delete and release spam messages addressed to them. For more information on these services, refer to the Installation Guide. Starting or Stopping ServicesAfter you have successfully installed IMSVA and configured the various settings, startthe services to begin scanning for malware and other threats. You may need to stopIMSVA services prior to performing an upgrade or backup function. Procedure 1. Go to System Status.

2. Under Managed Services Settings, click the Start or Stop button for the service(s)to start or stop. Selecting a Scan MethodIMSVA provides two scanning methods for detection of malware and other securitythreats. Procedure 1. Go to Policy > Scan Method. Getting Started 2-9 The Scan Method screen displays. 2. Select one of the following malware scanning methods. Smart Scan: Smart Scan leverages threat signatures that are stored in thecloud. When in Smart Scan mode, IMSVA uses the Smart Scan Agent Pattern tocheck for security risks. The Smart Scan Agent Pattern is updated daily byTrend Micro and delivers the same protection provided by conventional anti-malware and antispyware patterns. If the Smart Scan Agent Pattern cannotdetermine the reputation of a file, IMSVA queries the Smart ProtectionNetwork to provide up-to-date protection. Conventional Scan: Conventional scan leverages anti-malware andantispyware components stored locally. The Virus Pattern contains information that helps IMSVA identify the latestvirus/malware and mixed threat attacks. Trend Micro creates and releases newversions of the Virus Pattern several times a week, and any time after thediscovery of a particularly damaging virus/malware. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 2-10 Note Conventional Scan is the default scan method. 3. Optional: Use an HTTP proxy server to connect to the Smart Protection Network.Specify the following: Proxy server address Proxy server port User name Password 4. Click Save. Note IMSVA automatically restarts the Scan Service whenever you change your scanmethod settings. If Smart Scan is selected: IMSVA attempts to connect to the Smart Protection Network immediately afteryou click Save. If a connection is not established, IMSVA does not save yoursettings. Reselect a scan method and save your settings again. If there are ten (10) connection timeouts to the Smart Protection Network in three(3) minutes, IMSVA reverts to Conventional Scan. To use Smart Scan again, go tothe Scan Method screen and reselect Smart Scan. Note When IMSVA reverts to Conventional Scan, you can query system event logs foreach scanner's connection timeouts. If any scanner has frequent connection timeouts,check the network configuration of that scanner. For details on querying systemevent logs, see Querying System Event Logs on page 25-11. Getting Started 2-11 You can configure IMSVA to send notifications for unsuccessful attempts toconnect to the Smart Protection Network. For details on configuring notifications,see Notifications on page 27-1. 3-1 Chapter 3 User AccountsThis chapter explains how to add, configure, and manage user accounts. Topics include: Administrator Account Management on page 3-2 Adding Administrator Accounts on page 3-2 Editing or Deleting Administrator Accounts on page 3-5 Changing the Management Console Password on page 3-6 Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 3-2 Administrator Account ManagementTo reduce bottlenecks in administering IMSVA, you can delegate administrative tasks toother staff by creating new administrator accounts. After creating the accounts, assignthe desired permissions to the various areas of the management console. The default"admin" account has access to all IMSVA features. Adding Administrator Accounts Created accounts have three permission settings for IMSVA features: Full: Users have complete access to the features and settings contained in the menuitem. Read: Users can view features and settings contained in the menu item, but cannotmodify them. None: Users will not see the menu item, preventing them from viewing orconfiguring any of the settings in the menu item. Procedure 1. Go to Administration > Admin Accounts. The Admin Accounts screen appears. 2. Click Add. User Accounts 3-3 The Add Administrator Account screen appears, displaying the Authentication tab. 3. Specify Authentication settings: a. Select Enable account. b. Select an authentication type: IMSVA Authentication: Specify the user name, new password, and thenew password confirmation. The password must be between 4 and 32 alphanumeric characters. LDAP authentication: Specify the LDAP user name. 4.

Click the Permissions tab. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 3-4 The Permissions screen appears. 5. Specify Permissions settings: a. Select Full, Read, or None for each of the following access areas that appearon the IMSVA management console menu: Dashboard & System Status Cloud Pre-Filter Policy IP Filtering Reports Logs Mail Areas & Queues Administration Command Line Interface b. Click Save. User Accounts 3-5 Note Only the default IMSVA administrator account can add new administrator accounts.Custom administrator accounts cannot do so even if you assign full permission to theAdministration area. Custom administrator accounts with full administration rights can only change theirown IMSVA passwords. If you forget the default administrator account password,contact Trend Micro technical support to reset the password.

Editing or Deleting Administrator AccountsYou can change or delete the permissions of a custom administrator account wheneverthere is a revision of roles or other organizational changes. Editing Administrator Accounts Procedure 1. Go to Administration > Admin Accounts. The Admin Accounts screen appears. 2.

Click the account name hyperlink.

3. Make the required changes. 4. Click Save. Deleting Administrator Accounts Procedure 1. Select the check box next to the account to be removed. 2. Click Delete. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 3-6 3. Click OK. Note You can only delete custom administrator accounts, not the default IMSVAadministrator account. Changing the Management Console PasswordTrend Micro recommends periodically changing the password you use to access themanagement console.

WARNING! If you are still using the default password, Trend Micro strongly recommends that youchange the password immediately. Procedure 1. Go to Administration > Password. 2.

Specify the current password, the new password, and the new passwordconfirmation. User Accounts 3-7 Note A valid password can contain letters, numbers and the following characters: `~!@#$%^&*()[]{}+-|:'?/,.= _. The password must be between 4 and 32 alphanumeric characters.

3.

Click Save. 4-1 Chapter 4 Using the Configuration WizardThis chapter explains how to get IMSVA up and running using the configuration wizard. Topics include: Configuring System Settings on page 4-3 Configuring Deployment Settings on page 4-4 Configuring SMTP Routing on page 4-5 Configuring Notification Settings on page 4-6 Configuring the Update Source on page 4-8 Configuring LDAP Settings on page 4-10 Configuring Internal Addresses on page 4-14 Configuring Control Manager Server Settings on page 4-16 Activating the Product on page 4-18 Verifying Settings Summary on page 4-19 Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 4-2 Configuring IMSVA with the ConfigurationWizard IMSVA provides a configuration wizard to help you configure all the settings you needto get IMSVA up and running. Procedure 1. On the management computer, open a supported web browser. 2. Type the following URL (accept the security certificate if necessary): https://:8445 The Log On screen appears. 3. Select the Open Configuration Wizard check box. 4. Type the following default user name and password: User name: admin Password: imsva The Configuration Wizard screen appears. Using the Configuration Wizard 4-3 Configuring System Settings Procedure 1. Click Next. The Local System Settings screen appears. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 4-4 2. Modify the device host name, internal communication port, IP address, andnetmask if necessary. Also, configure your network settings and set the devicesystem time. Note The local system settings take effect immediately when you click the Next > button.If the IP address or time settings are changed, IMSVA will restart. Wait until IMSVAis online and then log on again. Configuring Deployment Settings Procedure 1.

Click Next. The Deployment Settings screen appears. 2.

Select Parent or Child. If this is the first device you are setting up, you must selectParent. You can configure additional child devices at a later time. Using the Configuration Wizard 4-5 Also, decide if you want to use the NTP service. Configuring SMTP Routing Procedure 1. Click Next. The SMTP Routing screen appears. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 4-6 2. Specify the incoming message settings. See Specifying Message Rules on page11-6. 3. Specify the message delivery settings. See Specifying Message Delivery Settings onpage 11-10. Configuring Notification Settings Procedure 1. Click Next. Using the Configuration Wizard 4-7 The Notification Settings screen appears. 2. Under Email Settings, configure the following: To address(es): Specify the recipient email addresses.

Sender's email address: Specify the email address to appear as the sender. Server name or IP address: Specify the Fully Qualified Domain Name(FQDN) or the IP address of the SMTP server that delivers email on thenetwork. SMTP server port: Specify the port number that IMSVA uses to connect tothe SMTP server. Preferred charset: IMSVA will use this setting to encode the notificationmessages.

Message header: Specify the text to appear at the top of the notification. Message footer: Specify the text to appear at the bottom of the notification. 3.

Under SNMP Trap, configure the following: Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 4-8 Note SNMP Trap is the notification message sent to the Simple Network ManagementProtocol (SNMP) server when events that require administrative attention occur. Server name: Specify the FQDN or IP address of the SNMP server. Community: Specify the SNMP server community name. Note Community is the group that computers and management stations running SNMPbelong to. To send the alert message to all SNMP management stations, specifypublic as the community name. For more information, refer to the SNMPdocumentation.

Configuring the Update Source Procedure 1. Click Next. Using the Configuration Wizard 4-9 The Update Source screen appears. 2. Configure the following update settings, which will determine from where IMSVAwill receive its component updates and through which proxy (if any) IMSVA needsto connect to access the Internet: OPTION DESCRIPTION Source Click Trend Micro ActiveUpdate server to receive updates directlyfrom Trend Micro. Alternatively, click Other Internet source andspecify the URL of the update source that will check the Trend MicroActiveUpdate server for updates. You can specify an update source ofyour choice or type the URL of your Control Manager serverhttp:///Tvcs Download/ActiveUpdate/, if applicable. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 4-10 OPTION DESCRIPTION ProxySettings Select the Use a proxy server for updates to patterns, engines,licenses, Web Reputation queries, Cloud Pre-Filter, and TrendMicro Email Encryption check box and configure the proxy type,server name, port, user name, and passwords. Configuring LDAP Settings Note Specify LDAP settings only if you will use LDAP for user-group definition, administratorprivileges, or End-User Quarantine authentication. Procedure 1. Click Next. Using the Configuration Wizard 4-11 The LDAP Settings screen appears. Trend Micro InterScan Messaging Security Virtual Appliance 9.0 Administrators Guide 4-12 2. Specify a meaningful description for the LDAP server. 3. Complete the following to enable LDAP settings: a. For LDAP server type, select one of the following: Domino Microsoft Active Directory Microsoft AD Global Catalog OpenLDAP Sun iPlanet Directory b. To enable one or both LDAP servers, select the check boxes next to EnableLDAP 1 or Enable LDAP 2. c. Specify the names of the LDAP servers and the port numbers they listen on.

d. Under LDAP cache expiration for policy services and EUQ services, specify anumber that represents the time to live next to the Time to Live in minutesfield. Using the Configuration Wizard 4-13 e. Under LDAP admin, specify the administrator account, its correspondingpassword, and the base-distinguished name. See the following table for aguide on what to specify for the LDAP admin settings. TABLE 4-1. LDAP Server Types LDAP SERVERLDAP ADMIN ACCOUNT(EXAMPLES) BASEDISTINGUISHED NAME (EXAMPLES) AUTHENTICATIONMETHOD ActiveDirectory WithoutKerberos: (UPN) ordomain\user1 With Kerberos: dc=domain,dc=com Simple Advanced (withKerberos) Active DirectoryGlobal Catalog WithoutKerberos: (UPN) ordomain\user1 With Kerberos: dc=domain,dc=com dc=domain1,dc=com (if mutipleunique domainsexist) Simple DocumentFormatSize Readme txt 170 KB Installation Guide pdf 7,100 KB Administrator's Guide pdf 11,461 KB Online Help html DocumentFormatSize Readme txt 67 KB High Availability Guide pdf 1,209 KB Installation Guide pdf 6,195 KB Administrator's Guide pdf 10,709 KB Online Help html DocumentFormatSize Readme txt 67 KB High Availability Guide pdf 1,244 KB Installation Guide pdf 6,365 KB Administrator's Guide pdf 11,226 KB Online Help html DocumentFormatSize Readme txt 23 KB High Availability Guide pdf 1,429 KB Installation Guide pdf 6,365 KB Administrator's Guide pdf 11,295 KB Online Help html