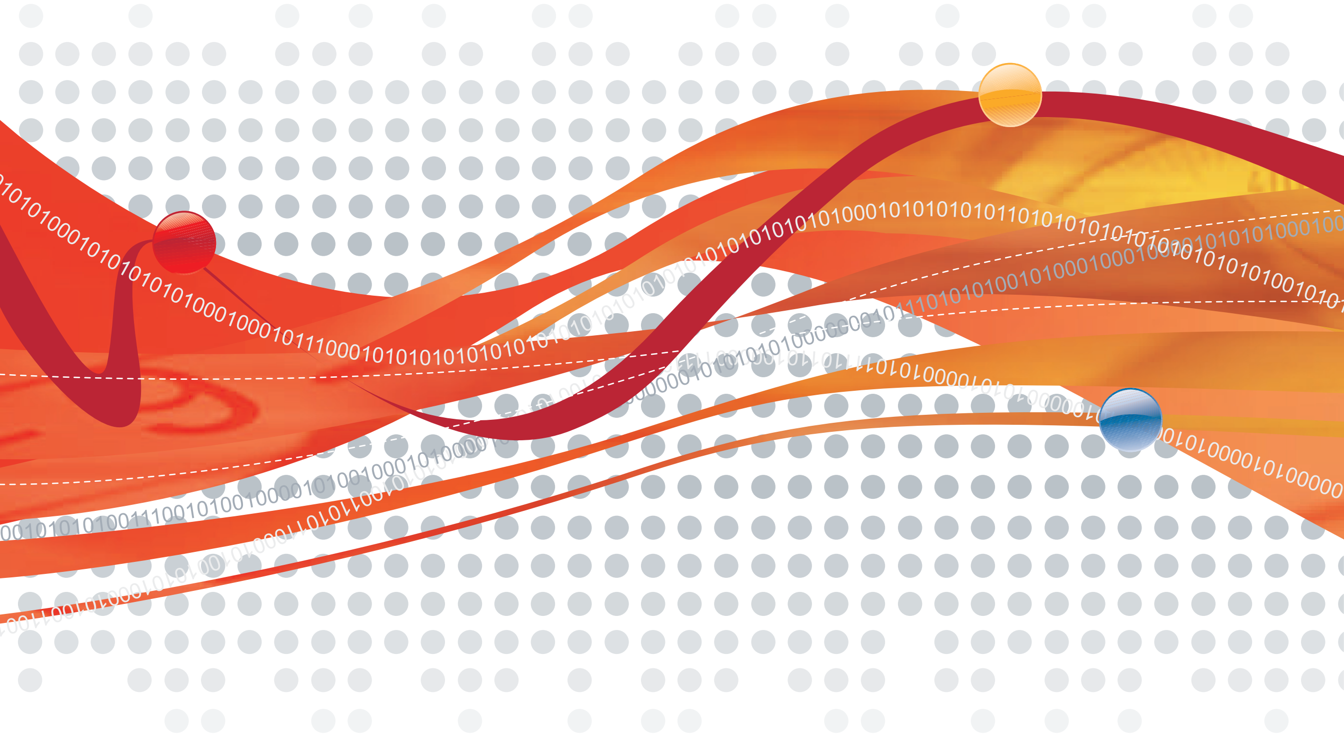
TREND MICRO™

InterScan™ Web Security Virtual Appliance 5.1

Antivirus and Content Security at the Web Gateway

Administrator's Guide



Web Security

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Installation Guide, which are available from Trend Micro's Web site at:

http://www.trendmicro.com/download/documentation/

Trend Micro, the Trend Micro t-ball logo, InterScan, TrendLabs, Trend Micro Control Manager, and Trend Micro Damage Cleanup Services are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2011 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Release Date: January 2011

Protected by U.S. Patent No. 5,951,698

The Administrator's Guide for Trend Micro is intended to provide in-depth information about the main features of the software. You should read through it prior to installing or using the software.

For technical support, please refer to the Technical Support and Troubleshooting chapter for information and contact details. Detailed information about how to use specific features within the software are available in the online help file and online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

`http://www.trendmicro.com/download/documentation/rating.asp`

Contents

Preface

Chapter 1: Introducing Trend Micro™ InterScan™ Web Security Virtual Appliance

Chapter 2: Deployment Wizard

Chapter 3: High Availability and Cluster Management

Chapter 4: Updates

Chapter 5: HTTP Configuration

Chapter 6: Policies and User Identification Method

Chapter 7: Configuring HTTP Scanning

Chapter 8: Access Quotas and URL Access Control

Chapter 9: URL Filtering

Chapter 10: FTP Scanning

Chapter 11: Command Line Interface Commands

Chapter 12: Reports, Logs, and Notifications

Chapter 13: Administration

Chapter 14: Testing and Configuring IWSVA

Appendix A: Contact Information and Web-based Resources

Appendix B: Mapping File Types to MIME Content-types

Appendix C: Architecture and Configuration Files

Appendix D: OpenLDAP Reference

Appendix E: Best Practices for IWSVA

Glossary of Terms

Preface

Preface

Welcome to the *Trend Micro™ InterScan™ Web Security Virtual Appliance 5.1 SP1 Administrator's Guide*. This guide provides detailed information about the InterScan Web Security Virtual Appliance (IWSVA) configuration options. Topics include how to update your software to keep protection current against the latest risks, how to configure and use policies to support your security objectives, configuring scanning, configuring URL blocking and filtering, and using logs and reports.

This preface describes the following topics:

- *IWSVA Documentation*
- *Audience*
- *Document Conventions*
- *About Trend Micro*

IWSVA Documentation

In addition to the *Trend Micro™ InterScan Web Security Virtual Appliance Administrator's Guide*, the documentation set for IWSVA includes the following:

- **Installation Guide**—This guide helps you get "up and running" by introducing IWSVA, assisting with installation planning, implementation, and configuration, and describing the main post-upgrade configuration tasks. It also includes instructions on testing your installation using a harmless test virus, troubleshooting, and accessing Support.
- **Online Help**—The purpose of online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online Help is accessible from the IWSVA Web console.
- **Readme file**—This file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and, release history.

  The latest versions of the Installation Guide, Administrator's Guide and readme file are available in electronic form at:

  http://www.trendmicro.com/download/
- **Knowledge Base**— The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, open:

  http://kb.trendmicro.com
- **TrendEdge**—A program for Trend Micro employees, partners, and other interested parties that provides information on unsupported, innovative techniques, tools, and best practices for Trend Micro products. The TrendEdge database contains numerous documents covering a wide range of topics.

  http://trendedge.trendmicro.com

Audience

The IWSVA documentation is written for IT managers and system administrators working in enterprise environments. The documentation assumes that the reader has in-depth knowledge of networks schemas, including details related to the following:

- HTTP and FTP protocols
- Database configuration
- VMware ESX administration experience when installing on VMware ESX

The documentation does not assume the reader has any knowledge of antivirus or Web security technology.

Document Conventions

To help you locate and interpret information easily, the IWSVA documentation uses the following conventions.

TABLE 1-1. Document Conventions

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations

TABLE 1-1. Document Conventions

CONVENTION	DESCRIPTION
WARNING!	Reminders on actions or configurations that should be avoided

About Trend Micro

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services. Founded in 1988, Trend Micro led the migration of virus protection from the desktop to the network server and the Internet gateway-gaining a reputation for vision and technological innovation along the way.

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impacts of risks to information, by offering centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop viruses and other malicious code from a central point, before they ever reach the desktop.

For more information, or to download evaluation copies of Trend Micro products, visit our award-winning Web site:

`http://www.trendmicro.com`

Chapter 1

Introducing Trend Micro™ InterScan™ Web Security Virtual Appliance

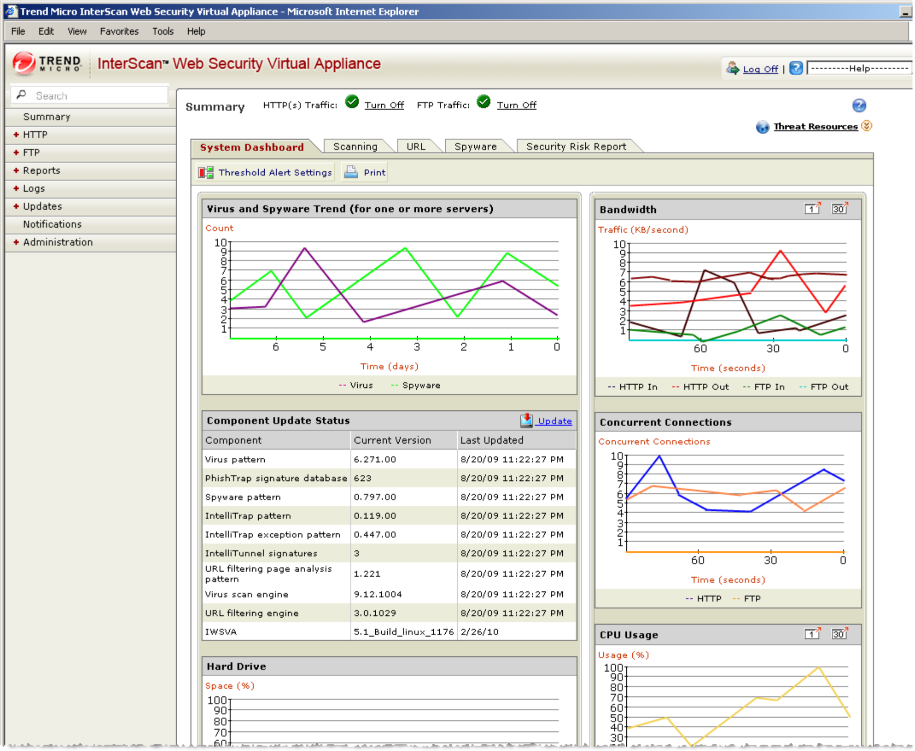
This chapter introduces the Trend Micro™ InterScan™ Web Security Virtual Appliance (IWSVA) and how it helps to ensure your organization's gateway security.

Topics in this chapter include the following:

- Web Traffic Security Risk Overview starting on page 1-2
- Hardware Specifications starting on page 1-4
- What's New starting on page 1-6
- Main Features starting on page 1-8

Web Traffic Security Risk Overview

Web traffic exposes corporate networks to many potential security risks. While most computer viruses enter organizations through messaging gateways, Web traffic is a common infection vector for new security risks. For example, "mixed risks," which take advantage of multiple entry points and vulnerabilities using HTTP to spread.



Component	Current Version	Last Updated
Virus pattern	6.271.00	8/20/09 11:22:27 PM
PhishTrap signature database	623	8/20/09 11:22:27 PM
Spyware pattern	0.797.00	8/20/09 11:22:27 PM
IntelliTrap pattern	0.119.00	8/20/09 11:22:27 PM
IntelliTrap exception pattern	0.447.00	8/20/09 11:22:27 PM
IntelliTunnel signatures	3	8/20/09 11:22:27 PM
URL filtering page analysis pattern	1.221	8/20/09 11:22:27 PM
Virus scan engine	9.12.1004	8/20/09 11:22:27 PM
URL filtering engine	3.0.1029	8/20/09 11:22:27 PM
IWSVA	5.1_Build_linux_1176	2/26/10

FIGURE 1-1. IWSVA Summary screen displays security risk information

Significant assessment, restoration, and lost productivity costs associated with outbreaks can be prevented. IWSVA is a comprehensive security product that protects HTTPS, HTTP, and FTP traffic in enterprise networks from viruses and other risks.

In addition to antivirus scanning, IWSVA also helps with other network security issues.

- Enhanced HTTP and FTP scan features provided by updated scan engine technology
- Web Reputation scrutinizes URLs before you access potentially dangerous Web sites, especially sites known to be phishing or pharming sites.
- URL filtering feature can allow, block, or monitor access to Web sites with content prohibited by your organization.
- HTTPS decryption feature allows encrypted traffic to pass through IWSVA scanning and filtering policies as “normal” HTTP traffic and verifies certificates from HTTPS servers.
- Applets and ActiveX security helps to reduce the risk of malicious mobile code by checking digital signatures at the HTTP(S) gateway, and monitoring applets running on clients for prohibited operations. With Applets and ActiveX security modules and URL Filtering now included in the IWSVA, these come at no extra cost to you.

Smart Search Support

The search field above the left menu allows users to find the features they need quickly, without navigating through the menu.

To use the Smart Search function:

1. Go to any page in IWSVA Web console.
2. In the Smart Search search field above the left-hand menu, begin to type the name of the feature to be located. (See *Figure 1-2*.)
3. Select the appropriate feature from the options provided in the drop-down list.
4. Press **Enter**.

   The page of your request feature displays.

Note: Smart Search is an instance-level feature. Passive nodes in High Availability environments will not be searched unless the administrator is logged into the passive member.

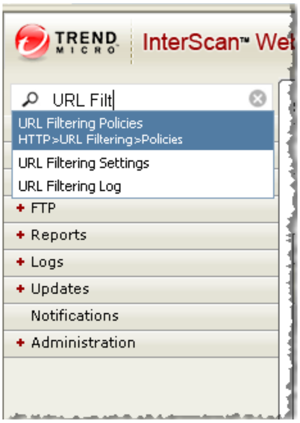


FIGURE 1-2. Smart Search available to find the location of features

Hardware Specifications

For a complete description of IWSVA server requirements, see the Installation Guide.

The minimum requirements specified provide enough resources to properly evaluate the product under light traffic loads. The recommended requirements specified provide general production sizing guidance.

For more detailed sizing information, refer to the *IWSVA Sizing Guide* at:

http://trendedge.trendmicro.com/pr/tm/te/document/IWSVA_Customer_Sizing_Guide_090930.pdf

Minimum Requirements:

- Single 2.0 GHz Intel™ Core2Duo™ 64-bit processor supporting Intel VT™ or equivalent
- 2GB RAM
- 12GB of disk space (IWSVA automatically partitions the detected disk space as required)
- Monitor that supports 1024x768 resolution with 256 colors or higher

Recommended Requirements:

- Dual 2.8 GHz Intel Core2Duo 64-bit processor or equivalent for up to 4000 users
- Dual 3.16 GHz Intel QuadCore™ 64-bit processor or equivalent for up to 9500 users
- 4GB RAM is recommended to support up to 4000 users
- 8GB RAM is recommended to support up to 9500 users
- 300GB of disk space or more for log intensive environments. IWSVA automatically partitions the detected disk space as per recommended Linux practices

For more information on capacity sizing, refer to the *IWSVA 5.0 Sizing Guide*.

Compatible Directory Servers

- Microsoft Active Directory™ 2003 and 2008
- Linux OpenLDAP Directory 2.2.16 or 2.3.39
- Sun™ Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)

Integration with ICAP 1.0-compliant Caching Devices

Cache servers help moderate Web traffic congestion and save bandwidth. The “retrieve once, serve many” method employed by cache servers permits integration with third-party applications such as virus scanning through IWSVA. An open protocol, Internet Caching Acceleration Protocol (ICAP), allows seamless coupling of caching and virus protection. IWSVA works with cache servers that support the ICAP 1.0 standard.

X-Authenticated ICAP Headers Support

IWSVA supports X-Authenticated ICAP Headers that are provided by supported ICAP clients, such as NetCache (5.6.2R1) and Blue Coat (SGOS 4.2.1.1). The X-Authenticated Headers come in two forms: X-Authenticated-User and X-Authenticated-Groups. The advantage of using X-Authenticated Headers is two-fold: first, it reduces LDAP query overhead in IWSVA and second, it allows ICAP clients to provide LDAP searches on LDAP servers with different schemas.

What’s New

IWSVA 5.1 SP1 is based on IWSVA 5.1 and provides the same malware protection, policy, logging and reporting capabilities.

The following features are new in this release.

High Availability

IWSVA supports high availability (HA) for service redundancy, providing active/passive failover in Transparent Bridge mode to ensure continuity in demanding business environments. HA in IWSVA is easily deployed through the Deployment Wizard and managed through the new cluster management feature. See High Availability Overview on page 3-2 for more information.

Cluster Management

The new cluster management feature allows administrators the ability to manage the HA cluster as a single entity by providing a common floating management IP address that is always associated with the active parent cluster member. The cluster management can be used to view and edit configuration settings as well as accessing the child member's specific configuration settings. See About Cluster Management on page 3-10 for more information.

Hardware Event Monitoring

The Hardware Status feature allows administrators to monitor critical hardware components and proactively set alerts about them. It monitors hardware information about fans, voltage, temperature, etc. on Intelligent Platform Management Interface (IPMI)-enabled devices. See Hardware Status on page 12-8 for more information.

Network Packet Capturing

Administrators can now analyze traffic with a new feature that allows packet captures for selected interfaces or a single interface. See Using Network Packet Capturing on page 13-21 for more information.

System Updates

Both OS updates and applications patches can be applied through the same Web console page. IWSVA differentiates between OS patches and the application patches and applies them appropriately. See System Updates on page 13-14 for more information.

Hyper-V Installation Supported

IWSVA now supports installation on Microsoft® Hyper-V® 2.0 with Windows Server 2008 R2 or later. The IWSVA installation for Hyper-V platforms supports forward proxy mode, WCCP mode, ICAP mode, and reverse proxy mode. See Appendix F of the *IWSVA Installation Guide* for more information.

Prevention of Brute Force Attacks against Password

IWSVA now supports the prevention of brute force attacks against passwords, focused on eliminating automated attacks in SSH. See Preventing Password Brute Force Attacks through SSH on page 11-2 for more information.

Advanced Reports and Management (ARM) Database Failover Support

If the ARM database is down or disconnected, IWSVA continues to operate.

Updates for URL Categories

Support for new URL filtering categories allows more granular URL access control.

Main Features

The following IWSVA features help you maintain HTTP and FTP gateway security.

Support for Multiple Trend Micro™ InterScan™ Web Security Virtual Appliance Installations

The method to fully administer multiple IWSVA devices from a single console is done through Trend Micro Control Manager (TMCM) and/or through Advanced Reporting and Management (ARM) for InterScan Web Security product family. TMCM provides the ability to manage multiple Trend Micro products and allows you to activate multiple IWSVA units from a central console. ARM provides centralized logging, reporting, and policy management for multiple IWSVA units and is only dedicated to the IWSVA products.

HTTP Virus Scanning

IWSVA scans the HTTP traffic flow to detect viruses and other security risks in uploads and downloads. HTTP scanning is highly configurable—for example, you can set the types of files to block at the HTTP gateway and how IWSVA scans compressed and large files to prevent performance issues and browser timeouts. In addition, IWSVA scans for many types of spyware, grayware, and other risks.

FTP Scanning

In addition to scanning FTP uploads and downloads, IWSVA can also block specified file types at the FTP gateway. To prevent performance issues, the FTP scanning module supports special configurations for compressed files and large files. Spyware and grayware scanning is also supported.

IWSVA FTP scanning can be deployed onto your environment in conjunction with another FTP proxy server, or IWSVA can act as an FTP proxy. To help ensure the security of Trend Micro™ InterScan™ Web Security Virtual Appliance, several security-related configurations are available to control access to IWSVA and its ports.

Improved Deferred Scanning for HTTP and FTP Large File Scans

To enhance the Web browsing experience, improved deferred scanning has been implemented. Instead of using a specified data size, IWSVA uses a percentage to define how much data is downloaded at a time. At most, every two seconds IWSVA sends a percentage of received data to the browser. The last chunk of data will not be larger than 4KB and is sent to the browser before the scan is finished. For the data download percentage, you can specify either 20, 40, 60, 80, or 100. The default percentage is 60.

For information on handling large files, see Handling Large Files on page 7-29.

Applets and ActiveX Security

To manage potential security issues in mobile code downloads from the Internet, IWSVA can block or allow Java applets and ActiveX controls. IWSVA includes its own certificate store to manage trusted and flagged certificates used to sign Java applets.

In addition, IWSVA can instrument Java applets so their operations are monitored while they run in client browsers. If a prohibited operation is performed, the client is notified and prompted to allow or deny the operation.

URL Filtering

With the URL Filtering option in IWSVA, you can set policies based on categories of URLs, such as “Adult”, “Gambling,” and “Financial Services.” When a user requests a URL, IWSVA first looks up the category for that URL and then allows, denies, or monitors access to the URL based on the policies you have set up. You can also define a list of approved URLs that will not be filtered.

Direct URL Filter Category Selection

From the Web Reputation database, IWSVA has access to over 80 categories of URLs, such as “gambling,” “games,” and “personals/dating.” You can also define your own custom categories.

Categories are contained in the following logical groups:

- Custom categories
- Network Bandwidth
- Internet Security
- Communications and Search
- Adult
- Business
- Lifestyle
- General

You can select all the categories of a specific group, or you can browse through the categories that comprise a group and select only certain categories (see URL Filtering Settings on page 9-8).

URL Filtering Category Mapping

Table 1-1 shows the URL Filtering Category mapping differences between IWSVA 5.1 and IWSVA 5.1 SP1.

TABLE 1-1. URL Category Mapping from IWSVA 5.1 to IWSVA 5.1 SP1

ID #	5.1 CATEGORY	5.1 SP1 CATEGORY
23=Internet Radio and TV	Computers/Bandwidth	Network Bandwidth
72=Pay to Surf	Computers/Bandwidth	Network Bandwidth
57=Peer-to-peer	Computers/Bandwidth	Network Bandwidth
56=Personal Network Storage/File Download Server	Computers/Bandwidth	Network Bandwidth
43=Photo Searches	Computers/Bandwidth	Network Bandwidth
70=Ringtones/Mobile Phone Downloads	Computers/Bandwidth	Network Bandwidth
71=Software Downloads	Computers/Bandwidth	Network Bandwidth

TABLE 1-1. URL Category Mapping from IWSVA 5.1 to IWSVA 5.1 SP1 (Continued)

ID #	5.1 Category	5.1 SP1 Category
69=Streaming Media/MP3	Computers/Bandwidth	Network Bandwidth
77=Adware	Computers/Harmful	Internet Security
80=Cookies	Computers/Harmful	Internet Security
81=Dialers	Computers/Harmful	Internet Security
79=Disease Vector	Computers/Harmful	Internet Security
82=Hacking	Computers/Harmful	Internet Security
83=Joke Program	Computers/Harmful	Internet Security
86=Made for AdSense	Computers/Harmful	Internet Security
78=Malware Accomplice Formerly “Virus Accomplice”	Computers/Harmful	Internet Security
84=Password Cracking	Computers/Harmful	Internet Security
75=Phishing	Computers/Harmful	Internet Security
73=Potentially Malicious Software	Computers/Harmful	Internet Security
39=Proxy Avoidance	Computers/Harmful	Internet Security
85=Remote Access Program	Computers/Harmful	Internet Security
76=Spam	Computers/Harmful	Internet Security
74=Spyware	Computers/Harmful	Internet Security
88=Web Advertisement	Computers/Harmful	Internet Security

TABLE 1-1. URL Category Mapping from IWSVA 5.1 to IWSVA 5.1 SP1 (Continued)

ID #	5.1 CATEGORY	5.1 SP1 CATEGORY
42=Blogs/Web Communications (Formerly Web Communications)	Computers/Communication	Communications and Search
51=Chat/Instant Messaging	Computers/Communication	Communications and Search
52=Email (Formerly "Email related")	Computers/Communication	Communications and Search
41=Internet Infrastructure (Formerly Infrastructure)	Computers/Communication	Communications and Search
24=Internet Telephony	Computers/Communication	Communications and Search
53=Newsgroups	Computers/Communication	Communications and Search
40=Search Engines/Portals	Social	Communications and Search
50=Social Networking	Computers/Communication	Communications and Search
89=Web Hosting	Computers/Communication	Communications and Search
16=Abortion	Adult	Adult
1=Adult/Mature Content	Adult	Adult
8=Alcohol/Tobacco	Adult	Adult
11=Gambling	Adult	Adult
25=Illegal Drugs	Adult	Adult

TABLE 1-1. URL Category Mapping from IWSVA 5.1 to IWSVA 5.1 SP1 (Continued)

ID #	5.1 CATEGORY	5.1 SP1 CATEGORY
9=Illegal/Questionable	Adult	Adult
5=Intimate Apparel/Swimsuit	Adult	Adult
26=Marijuana	Adult	Adult
6=Nudity	Adult	Adult
3=Pornography	Adult	Adult
4=Sex Education	Adult	Adult
10=Tasteless	Adult	Adult
14=Violence/Hate/Racism	Adult	Adult
15=Weapons	Adult	Adult
59=Auctions	Business	Business
32=Brokerage/Trading	Business	Business
21=Business/Economy	Business	Business
31=Financial Services	Business	Business
45=Job Search/Careers	Business	Business
60=Real Estate	Business	Business
58=Shopping	Business	Business
38=Computers/Internet	Business	General
67=Vehicles	Business	General
30=Activist Groups	Social	Lifestyle
44=Alternative Journals	General	Lifestyle

TABLE 1-1. URL Category Mapping from IWSVA 5.1 to IWSVA 5.1 SP1 (Continued)

ID #	5.1 CATEGORY	5.1 SP1 CATEGORY
19=Arts (Formerly Arts/ Entertainment)	Social	Lifestyle
22=Cult/Occult	Social	Lifestyle
29=Cultural Institutions	Social	Lifestyle
20=Entertainment (Formerly Arts/ Entertainment)	Social	Lifestyle
87=For Kids	General	LIfestyle
33=Games	Social	Lifestyle
62=Gay/Lesbian	Social	Lifestyle
63=Gun Clubs/Hunting	Social	Lifestyle
68=Humor (Formerly Humor/Jokes)	Social	Lifestyle
55=Personal Sites	Social	Lifestyle
47=Personals/Dating	Social	Lifestyle
18=Recreation/Hobbies	Social	Lifestyle
54=Religion	General	LIfestyle
64=Restaurants/Food (Formerly Restaurants/Dining/Food)	Social	Lifestyle
61=Society/Lifestyle	Social	Lifestyle
65=Sports	Social	Lifestyle

TABLE 1-1. URL Category Mapping from IWSVA 5.1 to IWSVA 5.1 SP1 (Continued)

ID #	5.1 CATEGORY	5.1 SP1 CATEGORY
76=Spam	Social	N/A
63=Sport Hunting and Gun Clubs	Social	N/A
66=Travel	Social	Lifestyle
38=Computers/Internet	General	General
27=Education	General	General
34=Government/Legal	General	General
37=Health	General	General
86=Made for AdSense sites (MFA)	General	N/A
35=Military	General	General
46=News/Media	General	General
36=Politics (Formerly Political)	General	General
49=Reference	General	General
48=Translators / Cached Pages (Formerly Translators (circumvent filtering)	General	General
67=Vehicles	N/A	General
90=Untested (Formerly Unrated)	General	General

Access Quota Policies

To set limits on client Web browsing, IWSVA allows configuring access quota policies. Clients can surf the Web up to their daily, weekly or monthly limit, after which further browsing is blocked until the configuration interval expires.

URL Access Control

IWSVA can reduce your server's scanning workload by not scanning content trusted URLs. Likewise, IWSVA can refuse requests to access content retrieved from URLs in order to prevent server resources from scanning content that you want to keep out of your organization (URL blocking).

IP Address, Host Name and LDAP Client Identification

IWSVA supports configuring policies for HTTPS decryption, HTTP virus scanning, Applets and ActiveX security, URL filtering, IntelliTunnel, and access quotas. The scope of policies can be configured using client IP address, host name or LDAP user or group name.

Server and Port Access Control Restrictions

To increase the security of IWSVA, access control lists limit server access to clients that you specify. Likewise, port access can be blocked to reduce the chance of access for malicious purposes.

Notifications

IWSVA can issue several types of notifications in response to program or security events. Administrator notifications are sent through email to the designated administrator contacts. User notifications are presented in the requesting client's browser. Both administrator and user notifications can be customized.

To work with network management tools, IWSVA can also issue several types of notifications as SNMP traps. IWSVA sends traps for security risk detections, security violations, program and pattern file updates, and service disruptions.

Because IntelliTrap is considered a type of security risk, it uses the same notifications as HTTP Scanning.

PhishTrap

Trend Micro helps protect LAN users from inadvertently giving away sensitive information as part of the of Internet fraud known as *phishing*. IWSVA protects you from phishing threats with a two-prong solution: PhishTrap and Web Reputation anti-phishing. From a remote database, Web Reputation retrieves the appropriate URL rating for a requested URL and then determines if it is a phishing threat.

While Web Reputation determines phishing threats based on the reputation of the requested URL, PhishTrap accomplishes this by using engine and pattern file technology. PhishTrap looks for phishing threats based on the signature file.

Note: You can use PhishTrap with or without Web Reputation. If PhishTrap is used without Web Reputation, you receive a basic level of protection. If PhishTrap is used with Web Reputation enabled, you receive a "layered" protection. When both features are enabled, the PhishTrap pattern match occurs before the Web Reputation query on a remote database.

Web Reputation

Web Reputation guards end-users against emerging Web threats. It can improve the Web surfing experience by enhancing Web filtering performance. Because a Web Reputation query returns URL category information (used by the URL Filtering module), IWSVA no longer uses a locally stored URL database.

Web Reputation also assigns reputation scores to URLs. For each accessed URL, IWSVA queries Web Reputation for a reputation score and then takes the necessary action, based on whether this score is below or above the user-specified sensitivity level.

IWSVA enables you to provide feedback on infected URLs, which helps to improve the Web Reputation database. This feedback includes product name and version, URL, and virus name. (It does not include IP information, so all feedback is anonymous and protects company information.) IWSVA also enables you to monitor the effectiveness of Web Reputation without affecting existing Web-access policies. Results are located in the URL Blocking Log and the Summary page (Security Risk Report tab).

For more Web Reputation information, see Specifying Web Reputation Rules on page 7-13 and Web Reputation Settings on page 7-15.

Anti-phishing and Anti-pharming Based on Web Reputation

IWSVA provides anti-phishing and anti-pharming through Web Reputation. Both of the features are enabled by default.

- Use anti-phishing to block Web access to phishing sites, which are meant to steal your private information.
- Use anti-pharming to block attempts to redirect you to imposter Web sites with the intention of stealing private information (usually financial-related).

IntelliTrap

IntelliTrap™ detects potentially malicious code in real-time, compressed executable files that arrive with HTTP data. Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides a heuristic evaluation of compressed files that helps reduce the risk that a virus compressed using these methods will enter a network through the Web.

For more IntelliTrap information, see IntelliTrap Pattern and IntelliTrap Exception Pattern Files on page 4-8 and About IntelliScan on page 7-24.

IntelliTunnel

IWSVA uses IntelliTunnel™ technology to block undesirable instant messaging (IM) and authentication connection protocols tunneled across port 80. It uses a dynamic, updatable pattern file to distinguish normal browser traffic from other protocols communicating over port 80.

For more information, see IntelliTunnel Security on page 7-44.

Easier Collection of System Information for Support Diagnosis

IWSVA provides the capability to collect logging and system configuration information more easily so that you can submit information quickly when contacting Trend Micro Support. The **Generate System Information File** button on the **Administration > Support > Support** screen allows you to collect this snapshot of IWSVA system information at the click of a button. See online help for complete details.

True File-type Blocking Within Compressed Files

IWSVA applies file-type blocking to the contents of a compressed file, such as a zip file. Therefore, a policy meant to block executables also blocks any zip file that contains an executable.

For more information, see About True-file Type on page 7-24.

Real-time Statistics and Alerts

IWSVA provides dynamic statistics where the administrator can view the "real-time" information about the IWSVA system. Real-time statistics are displayed as graphs and tables in the System Dashboard tab of the Summary page. These statistics include the following:

- Hard Drive

  Hard drive statistics are static and are only updated when you open the Summary page.
- Bandwidth
- Concurrent Connections
- CPU Usage
- Physical Memory Usage

For more information, see Real-time Statistics on page 12-2.

Optionally, IWSVA can be configured to send information to Trend Micro's Advanced Reporting and Management (ARM) for InterScan Web Security products for central logging, reporting, and policy management. ARM provides high-performance reporting with many additional report types and advanced features such as report drilldown, activity monitoring, dynamic dashboarding, and much more.

Configurable Threshold Warning

IWSVA allows a configurable threshold warning to be set when virus and spyware traffic, database and hard disk size, or bandwidth utilization exceeds the specified threshold. For more information, see Enabling Threshold Alerts Notifications on page 12-50.

Reverse Proxy Support

IWSVA is usually installed close to clients to protect them from Internet security risks. However, IWSVA also supports being installed as a reverse proxy to protect a Web server from having malicious programs uploaded to it. As a reverse proxy, IWSVA is installed close to the Web server that it protects. IWSVA receives client requests, scans all content and then redirects the HTTP requests to the real Web server.

For more information, see Reverse Proxy on page 5-9.

Logs and Reports

IWSVA includes many pre-configured reports to provide a summary of your gateway security status. Reports can be run for a specific time period and customized to only provide information about clients that you are interested in. The following lists the main report classes:

- Violation event reports
- Traffic reports
- Spyware/grayware reports
- Cleanup reports
- URL filtering category reports
- Individual user reports

Reports are generated from log information in the database. IWSVA writes log information to text-only logs, text and database logs, or database-only logs.

Reports can be generated on demand or scheduled on a daily, weekly, or monthly basis. Log and report data can be exported to comma-separated value (CSV) files for further analysis. To prevent logs from consuming excessive disk space, a scheduled task deletes older logs from the server.

For more information, see Reports, Logs, and Notifications on page 12-1.

Optionally, IWSVA can be configured to send information to Trend Micro's Advanced Reporting and Management for InterScan Web Security (ARM) product for central logging, reporting, and policy management. ARM provides high-performance reporting with many additional report types and advanced features such as report drilldown, activity monitoring, dynamic dashboarding and much more.

Additional Reporting Information

IWSVA reports Web Reputation, anti-pharming, and anti-phishing on the Summary page and on URL blocking reports:

- **Summary Page: Security Risk Report tab:** Accumulated number for the detected pharming sites in a week and 28 days can be displayed in the Security Risk Report like other Web threats. Files detected by IntelliTrap are counted as a separate risk in the report.
- **Reports (Real-time and Scheduled):** Blocked pharming sites are reported in the following reports because pharming activity is logged in the URL Blocking Log:
  - Most blocked URLs
  - Most blocked URLs by day of the week
  - Most blocked URLs by hour

IWSVA reports IntelliTrap activity in the following areas:

- **Summary Page: Scanning tab:** Files detected by IntelliTrap are listed in the "Scanning results for" with its frequency.

For more information, see Reports, Logs, and Notifications on page 12-1.

Integration with Cisco WCCP

IWSVA supports Web Cache Communication Protocol (WCCP) version 2, a protocol defined by Cisco Systems. See your Cisco product documentation for more information on the protocol.

The following are the benefits gained when IWSVA supports WCCP:

- Transparency of deployment without endpoint configuration
- High availability and load balancing between multiple IWSVA systems
- Automated load balancing re-configuration when adding or removing IWSVA appliances
- Support Cisco router, switch, and firewall implementations of the protocol

The WCCP implementation for IWSVA is compatible with Cisco routers, switches, PIX firewalls, and ASA security devices.

Trend Micro recommends using the following Cisco IOS versions when configuring WCCP with IWSVA:

- 12.2(0) to 12.2(22). Avoid using releases 23 and above within the 12.2 family
- 12.3(10) and above. Avoid using releases 0-9 in the 12.3 family
- IOS 15.1(1)T3 or above

Trend Micro recommends using version 7.2(3) and above for the Cisco PIX firewall and avoiding version 7.2(2).

Non-Cisco devices that support WCCP version 2 have not been explicitly tested by Trend Micro. Therefore, interoperability cannot be guaranteed.

Command Line Interface

IWSVA provides a native Command Line Interface (CLI) to perform system monitoring, system administration, debug, troubleshooting functions and more through a secure shell or a direct console connection.

IWSVA's CLI uses industry standard syntax to provide a familiar interface for configuring the appliance. For security, IWSVA allows administrators to access the CLI through the console or an SSH connection only. You can enable this feature in the IWSVA Web console.

HTTPS Decryption

IWSVA closes the HTTPS security loophole by decrypting and inspecting encrypted content. You can define policies to decrypt HTTPS traffic from selected Web categories. While decrypted, data is treated the same way as HTTP traffic to which URL filtering and scanning rules can be applied.

Secure Shell (SSH) Configuration in Web Console

IWSVA allows you to enable SSH (Secure Shell) to allow administrators to access the CLI from a remote location. SSH is a network protocol that allows two network devices to exchange data in a secured connection. SSH replaces Telnet, which sends data (including passwords) in clear text.

Per-policy Exception

For granular control of policies, IWSVA allows approved URL and file name lists to be defined on a per policy basis. In addition, IWSVA provides the option to bypass virus scans and compressed file handling actions for the approved lists.

Compressed File Handling Actions

IWSVA allows you to select various actions (block, pass, quarantine) when compressed file settings are violated.

Custom Category

For flexible URL filtering, IWSVA allows the creation of new categories to satisfy the need for more Web site categories than is provided by the URL Filtering module.

URL Monitoring Mode

As an enhanced feature for URL Filtering, IWSVA supports a monitor filtering action. With the monitor action, IWSVA allows access to specify categories and records the access event in the logs - users do not receive a block message.

Reporting

IWSVA provides local and centralized reporting (through the optional Advanced Reporting & Management module) that provides flexible reporting capabilities. Reports can be produced and printed, saved or exported in various formats (PDF and CSV), sent to one or more email accounts, or viewed on the screen. With the optional Advanced Reporting & Management module, real-time reporting is enhanced with drill-down reporting, near real-time monitoring of critical user activity, and over 160 data views and reports to meet many different reporting needs.

Web Page Analysis

IWSVA supports real-time content analysis to check for malicious content in a Web page and automatically adjusts the reputation score to catch zero-day threats and new attacks.

Safe Search Engine

IWSVA supports the Safe Search feature provided by search engines' filtering mechanism (such as Google.com and Yahoo.com). Safe Search is used to specifically filter adult sites and content from the search results and helps protect children and other users from being exposed to adult material.

User/group Name Authentication in Transparent Mode (WCCP and Bridge mode)

IWSVA supports user/group name authentication in transparent mode (WCCP and Bridge mode) in addition to forward proxy mode.

White List for User/group Name Authentication

IWSVA supports IP white list, which is based on a range of IP addresses, to bypass user/group name authentication. With this feature, back-end services which do not need to do authentication can be bypassed based on IP addresses or IP range.

In addition, IWSVA supports Global Trusted URLs list to bypass authentication for URLs that do not need authentication. IWSVA does not filter or scan the contents for URLs in this list.

Network Interface Configuration and PING Management

IWSVA supports a dedicated (also known as out-of-band) management interface that does not carry user data. You can configure both the data and management interface settings in the Web console. In addition, you can configure the PING option for each interface.

System Event Logs

IWSVA provides system event logs that records system configuration changes, maintenance activities (such as system restart), and service activities.

Syslog Support

To provide enterprise-class logging capabilities, IWSVA allows sending logs using the syslog protocol (default UDP port 514) to multiple external syslog servers in a structured format.

System Shutdown or Restart

For convenient system maintenance, IWSVA supports system shutdown or reboot and IWSVA service restart through the Web console. These maintenance activities are also recorded in system event logs for record keeping.

Configuration Backup and Restore

The configuration backup and restore feature allows you to migrate settings and data files from supported IWSA, IWSS, and IWSVA products to IWSVA 5.1 SP1. In addition, you can also perform regular backups of existing IWSVA 5.1 SP1 configuration and data.

License Management in Control Manager

With improved TMCM 5.0 integration, you can activate or renew activation codes for IWSVA from Control Manager. This is a convenient feature if you are managing multiple IWSVA servers in your company network.

Manual Component Update Button

In addition to scheduled component updates, you can click the manual update button to have IWSVA perform an immediate update of all components.

Advanced Reporting and Management Integration

Trend Micro Advanced Reporting and Management (ARM) provides a high-performance, off-box reporting solution. ARM is based on new advanced database technology, which greatly enhances the current InterScan Web Security product reporting capabilities and provides advanced features, such as dynamic dashboard, drill-down reporting, custom reporting and real-time, problem-solving capabilities.

Deployment Wizard

After installation, a Deployment Wizard opens automatically on first login to Web console to help the user set up IWSVA according to the user's deployment environment. See Chapter 2 - Deployment Wizard starting on page 2-1 for details.

Fail Open/LAN Bypass

Fail open/LAN bypass cards are now configured using CLI commands instead of entering the shell to run batches of scripts. See LAN-bypass Function on page 2-39.

Notification Message Enhancement

Rich context notification messages, instead of plain text, help administrators or end users easily understand the prompted notifications. See Introduction to Notifications on page 12-37 for details.

Smart Search

The Smart Search field above the left menu helps users navigate the GUI and find features. Typing a feature name directs you to the appropriate feature page in the GUI. See Smart Search Support on page 1-3 for details.

URL Filtering Access Warning Mode

URL Filtering now offers a warning mode. A notification informs the user about a violation in company policy before accessing a URL in a prohibited category. See Creating a New Policy on page 9-5 and Configuring URL Access Warning Notifications on page 12-53.

LDAP Integration Policy Improvement

LDAP transparent authentication improvement combines the Domain Controller query and the Windows client query. It helps to reduce end-user authentication pop-ups. See Transparent Identification on page 6-10.

IWSVA also offers enhanced LDAP and AD 2008 support.

Product License

IWSVA is activated by one Activation Code (AC) instead of three separate ACs as done in previous versions.

Content Cache

Web content caching is the caching of Web objects (for example, HTML pages, images) to reduce bandwidth usage, server load, and perceived lag. A Web cache stores copies of objects passing through it. Subsequent duplicate requests may be satisfied from the cache if certain conditions are met. The Content Cache capability provides users who access the Web through IWSVA with a quicker experience while saving bandwidth. See Using the Content Cache on page 7-18 for details.

HTTPS Scanning

HTTPS scanning now supported in transparent mode (bridge and WCCP) with upstream proxies. A new driver adds support of SSL hardware accelerator cards to perform all of the high computational calculations needed for HTTPS. This card saves the general purpose CPU cycles for other IWSVA functions– such as content inspection. See HTTPS Accelerator Card Support on page 7-7 for details.

X-Forwarded-For Header

IWSVA now parses the “X-Forwarded-For” header to obtain the original client IP address or it can add the “X-Forwarded-For” header for the upstream proxy. See X-Forwarded-For HTTP Headers on page 7-36 for details.

Administration and Management

- Administrators can create Access Control Lists that restrict Admin UI access to specific IP addresses or IP address ranges of the separate management interface. See Configuring Internet Access Control Settings on page 5-13.
- Simpler, more unified installation process leveraged by IWSVA.
- VMware tools, installed automatically when IWSVA is installed, supporting VMware versions 3.5 and 4.0

Virus Scan Technology Enhancement

Features added from the newest Virus Scan technology (VSAPI 9.0) include blocked file type enhancements, including:

- Preventing newer malware applications from bypassing VSAPI's True File Type identification
- Offering a clear way to display the blocked file types
- Expands the number of true file types supported by VSAPI 9.0 technology, which allows administrators to specify specific MIME-type files to be skipped during scanning to improve performance and usability. See Mapping File Types to MIME Content-types on page B-1 for more information.

Chapter 2

Deployment Wizard

The contents of this chapter help to guide you through the deployment process as you configure InterScan Web Security Virtual Appliance (IWSVA) for your network.

Topics in this chapter include the following:

Overview of the Deployment Wizard

The Deployment Wizard and the change password dialog box both display automatically at first login.

Note: **-1.)** If you are using a pop-up blocker, the Deployment Wizard and the password change dialog box will not appear.
-2.) Trend Micro recommends changing your admin password when prompted at first logon before using the Deployment Wizard.

The Deployment Wizard walks you through the deployment process. It is invoked automatically the first time administrators log into the IWSVA Web console. It can be manually invoked from **Administration > Deployment Wizard** at any time to review or change settings.

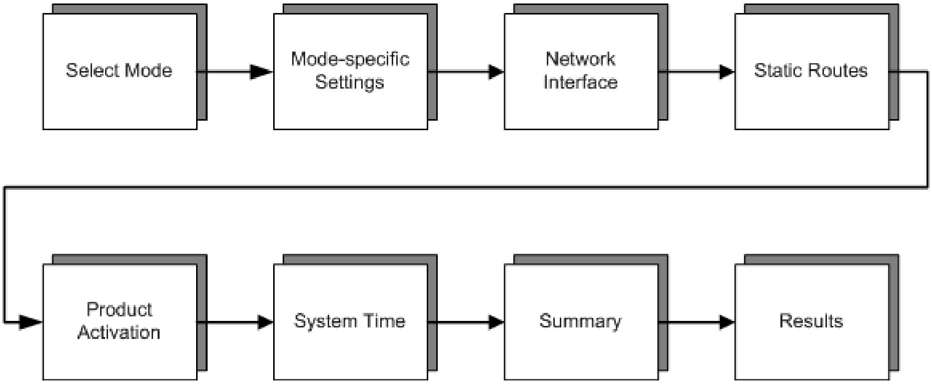


FIGURE 2-1. Deployment Wizard flow

Mode Selection

IWSVA can be deployed in different modes, depending on your network security needs. For more information on which mode to select, see the Deployment Primer in Chapter 2 of the *IWSVA Installation Guide.*

The Deployment Wizard allows you to configure IWSVA in one of seven modes.

- Transparent Bridge Mode on page 2-3
- Transparent Bridge Mode - High Availability on page 2-4
- Forward Proxy Mode on page 2-8
- Reverse Proxy Mode on page 2-10
- ICAP Mode on page 2-11
- Simple Transparency Mode on page 2-12
- Web Cache Coordination Protocol (WCCP) Mode on page 2-14

Transparent Bridge Mode

IWSVA acts as a bridge between network devices such as routers and switches. IWSVA scans passing HTTP and FTP traffic without the need to modify browser or network settings. This is the easiest deployment mode with traffic scanned in both directions.

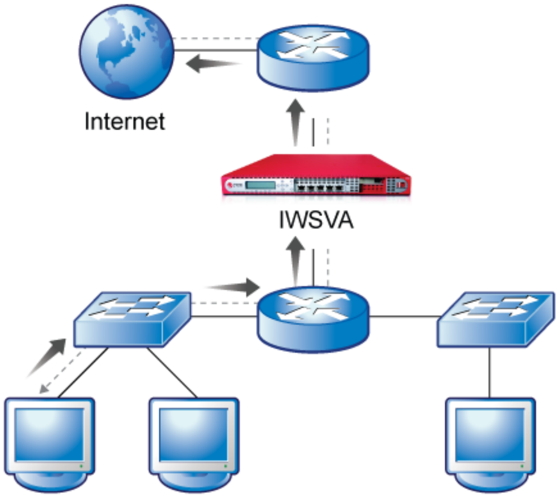


FIGURE 2-2. Transparent Bridge Mode

The additional dependency for this deployment mode is two network interface cards per transparent bridge segment protected with IWSVA. Trend Micro recommends the following network cards be used to ensure maximum compatibility:

- Broadcom NetXtreme Series
- Intel Pro/1000 PT Dual Port Server Adapter
- Intel Pro/1000 MF Dual Port Fiber

Depending on the number of NIC cards detected, the Transparent Bridge Mode option might not be available. For Transparent Bridge Mode deployments, there must be a minimum of two detectable network cards in the system.

Note: For more information on setting up IWSVA in Transparent Bridge mode, see Network Configuration and Load Handling on page 5-11.

To deploy IWSVA in Transparent Bridge mode:

1. Go to **Administration > Deployment Wizard**.

   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Transparent Bridge Mode** radio button on the Deployment Mode page.
4. Click **Next**.
5. Go to Network Interface on page 2-24 to continue.

Note: Transparent Bridge Mode for a single node requires no mode-specific settings. For more information on setting up IWSVA, see Network Configuration and Load Handling on page 5-11.

Transparent Bridge Mode - High Availability

The IWSVA High Availability (HA) solution currently supports active/passive pairs utilizing the Transparent Bridge mode. To deploy an IWSVA cluster, each IWSVA unit must use a separate management interface.

The Transparent Bridge Mode - High Availability for HA deployment requires at least the four following network interfaces cards (NICS) for cluster deployment:

- Two for bridge data interfaces
- One for the HA interface
- One for the separate management interface

Note: For more information about high availability and cluster management, see *High Availability and Cluster Management* starting on page 3-1.

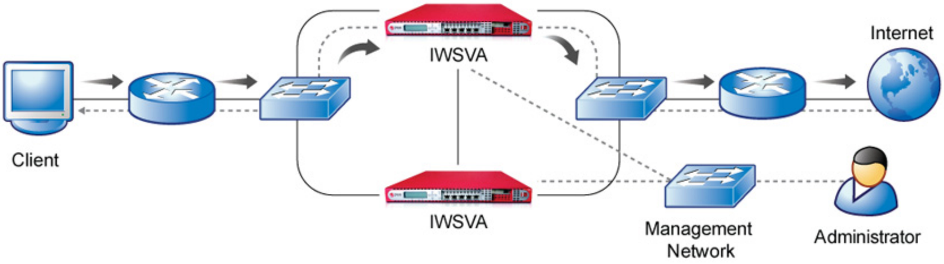


FIGURE 2-3. Transparent Bridge Mode - High Availability

Note: IWSVA only supports two HA nodes in a single HA cluster.

Using the Deployment Wizard, you can either:

- Create a New Cluster on page 2-6
- Join an Existing Cluster on page 2-7

About Cluster IP Addresses

The Cluster IP address is the floating IP address of the management port of the cluster. Users access this IP address through the Web console or the CLI to manage the cluster. The floating IP address floats in the cluster. If a switchover occurs, the floating IP address of cluster (the cluster IP address) always points to the parent device.

About Weighted Priority Election

Enabling Weighted Priority Election allows the device with the highest weight to always be selected as the parent member. Disabling the Weighted Priority Election process means the current parent member remains the parent member even when a new cluster member with a higher weight is added into the cluster.

The weight is the user-defined priority of the member in the cluster. If two members have the same weight assigned, there will still be one parent and one child, but the selection of the parent member is based on an internal algorithm. If you enable Weighted Priority Election, cluster members are prohibited from having equal weights.

Create a New Cluster

To create a new cluster:

1. Go to **Administration > Deployment Wizard**.

   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Transparent Bridge Mode - High Availability** option on the Deployment Mode page.
4. Click the **New Cluster** option.
5. Click **Next**.
6. Set the Cluster settings, which include:
   a. Type a cluster name.
   b. Type an (optional) cluster description.
   c. Type the Cluster IP address. See About Cluster IP Addresses on page 2-5 for details.
   d. Select Enable or Disable from the Weighted Priority Election drop-down list.

      Note: For more information on Weighted Priority Election, see About Weighted Priority Election on page 2-6.

- If enabled, the HA pair launches an election to choose the maximum-weighted machine.
- If disabled, the HA pair only launches an election when the current active (primary) machine is not available.

Note: The HA mode displays as Active/Passive and the Deployment mode always shows Bridge to indicate Transparent Bridge Mode - High Availability.

e. Using the information in the Interface Status section, select the HA Interface from the drop-down list (eth0, eth1, eth2, eth3, etc.)

Active and passive IWSVAs are connected directly though the HA or "Heartbeat" interface. The interface, labeled H in the interface status graphic, has two functions:

- Active and passive virtual appliances send a package per second to notify each other they are up and running.
- The interface is used in the synchronization process.

See *Figure* on page 2-27 and *Table 2-2* on page 2-27 for more information on using the Interface Status graphic. Also see Determining the Status of the Interfaces on page 2-26.

f. Enter the Weight value. (Default 128)

- The member with the higher weighting has higher priority and becomes the parent member.

7. Click **Next**.

8. Set up the Network Interface on page 2-24 to continue the deployment.

Join an Existing Cluster

To join an existing cluster:

1. Go to **Administration > Deployment Wizard**.

Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Transparent Bridge Mode - High Availability** option on the Deployment Mode page.
4. Click the **Join a Cluster** option.
5. Click **Next**.
6. Set the Cluster settings, which include:
    a. Using the information in the Interface Status section, select the HA Interface from the drop-down list (eth0, eth1, eth2, eth3, etc.)

    Active and passive IWSVAs are connected directly though the HA or "Heartbeat" interface. The interface, labeled H in the interface status graphic, has two functions:

    - Active and passive virtual appliances send a package per second to notify each other they are up and running.
    - The interface is used in the synchronization process.

    See *Figure* on page 2-27 and *Table 2-2* on page 2-27 for more information on using the Interface Status graphic. Also see Determining the Status of the Interfaces on page 2-26.

    b. Enter the Weight value. (Default 64)
7. Click **Next**. A progress bar displays, showing connection to the existing cluster.
8. Review the cluster information page that displays after connecting to the cluster and click **Next**.
9. Set up the Network Interface on page 2-24 to continue the deployment.

Forward Proxy Mode

IWSVA acts as an upstream proxy for network clients. Client browser settings must be configured to redirect traffic to IWSVA. IWSVA scans HTTP and FTP traffic and there is no separate need for another dedicated proxy server. Content is scanned in both the inbound and outbound directions.

Forward Proxy Mode also provides the following additional capabilities:

- Forwards all traffic to another upstream proxy server
- Participates in a proxy chain configuration with other proxy servers and supports X-Forwarded-For functionality

Note: For more information on setting up IWSVA in Forward Proxy mode, see Network Configuration and Load Handling on page 5-11.

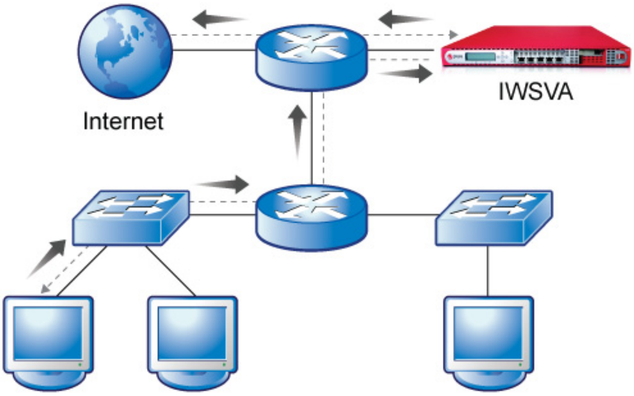


FIGURE 2-4. Forward Proxy Mode

To deploy IWSVA in Forward Proxy Mode:

1. Go to **Administration > Deployment Wizard**.

   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Forward Proxy Mode** radio button on the Deployment Mode page.
4. Click **Next**.
5. Go to Mode-specific Settings on page 2-15 to continue.

Reverse Proxy Mode

IWSVA is deployed in front of a Web server. IWSVA scans HTTP and FTP content from the clients that are uploaded to a web server as well as content that is downloaded from the Web server to the clients and helps secure the Web server.

Note: For more information on setting up IWSVA in Reverse Proxy mode, see Network Configuration and Load Handling on page 5-11.

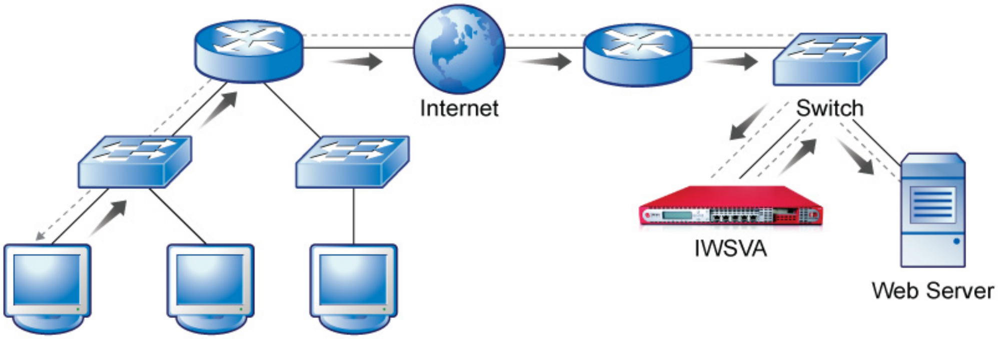


FIGURE 2-5. Reverse Proxy Mode

To deploy IWSVA in Reverse Proxy Mode:

1. Go to **Administration > Deployment Wizard**.

   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Reverse Proxy Mode** radio button on the Deployment Mode page.
4. Click **Next**.
5. Go to Mode-specific Settings on page 2-15 to continue.

ICAP Mode

IWSVA acts as an ICAP proxy and accepts ICAP connections from an ICAP v1.0 compliant cache server. Cache servers can help reduce the overall bandwidth requirements and reduce latency by serving cached content locally. IWSVA scans and secures all content returned to the cache server and to the clients.

Note: To enable and configure ICAP mode, see Network Configuration and Load Handling on page 5-11 and Setting Up IWSVA ICAP on page 2-41.

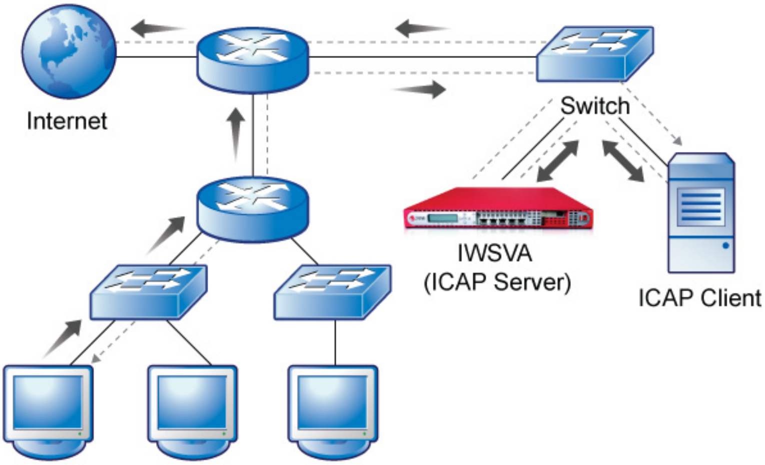


FIGURE 2-6. **ICAP Mode**

Deploying IWSVA in ICAP Mode in the Deployment Wizard

To deploy IWSVA in ICAP mode:

1. Go to **Administration > Deployment Wizard**.

   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **ICAP Mode** radio button on the Deployment Mode page.
4. Click **Next**.
5. Go to Mode-specific Settings on page 2-15 to continue.

Simple Transparency Mode

IWSVA's Forward Proxy Mode supports simple transparency with popular Layer 4 load balancing switches and provides HTTP scanning without the need to modify the client's browser settings.

Note: For more information on setting up IWSVA in Simple Transparency mode, see Network Configuration and Load Handling on page 5-11.

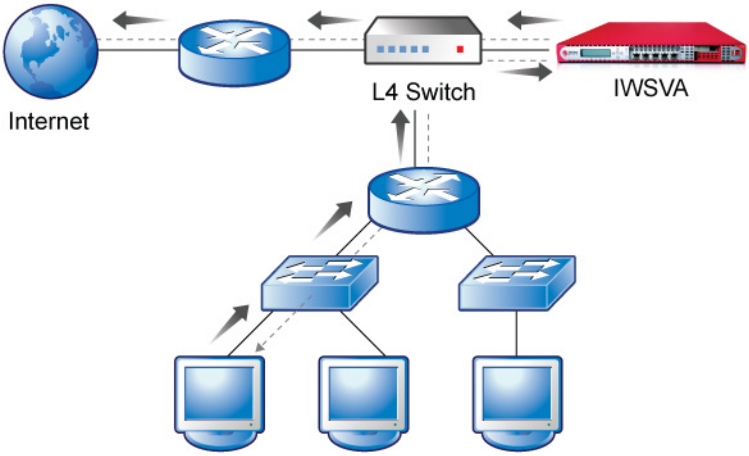


FIGURE 2-7. Simple Transparency Mode

To deploy IWSVA in Simple Transparency Mode:

1. Go to **Administration > Deployment Wizard**.

Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **Simple Transparency Mode** radio button on the Deployment Mode page.
4. Click **Next**.
5. Go to Mode-specific Settings on page 2-15 to continue.

Web Cache Coordination Protocol (WCCP) Mode

IWSVA works with Cisco's WCCP protocol to provide content scanning for Web and FTP traffic without the need to modify client configurations and allows redundancy and saleability to be designed into the architecture without additional hardware.

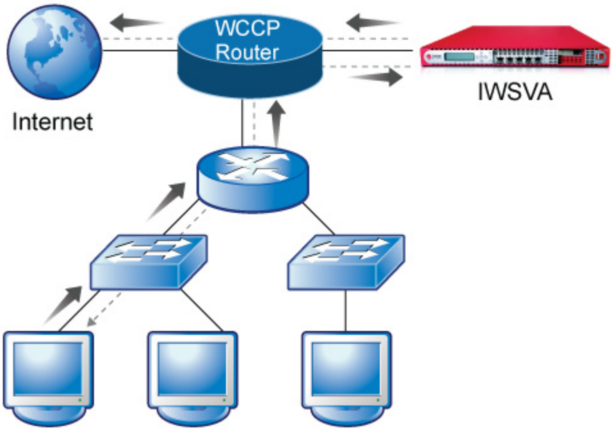


FIGURE 2-8. WCCP Mode

Note: For more information on setting up your WCCP server for use with IWSVA, see Network Configuration and Load Handling on page 5-11 and your Cisco product documentation.

To deploy IWSVA in WCCP Mode:

1. Go to **Administration > Deployment Wizard**.

   Note: The Deployment Wizard launches automatically the first time an administrator logs in.

2. Click **Start** on the Welcome page.
3. Click the **WCCP Mode** radio button on the Deployment Mode page.

4. Click **Next**.
5. Go to Mode-specific Settings on page 2-15 to continue.

Mode-specific Settings

Some deployments modes have settings that are unique to that mode. The second step in deployment Wizard allows you to configure those settings. Transparent Bridge Mode has no mode specific settings.

TABLE 2-1. Mode-specific Settings

MODE	MODE-SPECIFIC SETTINGS	PAGE
Transparent Bridge	None	N/A
Transparent Bridge for HA	New: • Cluster settings • Weighted Priority Election (Y/N) • HA Interface • Weight Existing: • HA Interface • Weight	New: 2-6 Existing: 2-7
Forward Proxy	Proxy settings	2-15
Reverse Proxy	Proxy settings	2-15
ICAP	ICAP settings	2-20
Simple Transparency	Transparency settings	2-22
WCCP	WCCP settings	2-23

Proxy Settings

Proxy settings must be configured if you are installing in the following modes:

- Forward Proxy, Standalone Mode - See Standalone Proxy Mode Settings on page 2-16
- Forward Proxy, Upstream Proxy Mode -See Upstream Proxy (Dependent) Mode Settings on page 2-17
- Reverse Proxy Mode - See Reverse Proxy Settings on page 2-19

Forward Proxy Mode

Depending on your network configuration, you can either specify:

- Standalone Proxy Mode Settings on page 2-16
- Upstream Proxy (Dependent) Mode Settings on page 2-17

Standalone Proxy Mode Settings

To configure the proxy settings for Standalone Mode:

1. Select the **Forward Proxy mode** radio button on the Deployment Mode page.

   See Forward Proxy Mode on page 2-8 for details.
2. Click **Next**.
3. Follow the configuration recommendations in *Table 2-1*.

TABLE 2-1. Standalone settings in Forward Proxy Mode

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections	8080
Enable upstream proxy (check box)	Enable / disable upstream proxy	Leave unchecked if you do not use another proxy device upstream of IWSVA.

TABLE 2-1. Standalone settings in Forward Proxy Mode

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
Enable guest account	Guest mode provides a secondary proxy port that uses the Guest Policy and simplifies deployment without the need to authenticate guests before giving them access to the Internet. In order to enable Internet connectivity to network users who are not in the LDAP directory and apply guest policies, this setting opens a guest port for Web clients to communicate with IWSVA.	Enable and accept the default port of 8081 if you want to support the secondary Guest proxy port. The Guest port can be changed if needed.
Anonymous FTP over HTTP	The email address passed to FTP sites	Change to an appropriate address

4. Click **Next**.
5. Set up the Network Interface on page 2-24 to continue the deployment.

Upstream Proxy (Dependent) Mode Settings

To configure the Proxy Settings for Upstream Mode:

1. Select the **Forward Proxy mode** radio button on the Deployment Mode page.

   See Forward Proxy Mode on page 2-8 for details.
2. Click **Next**.

3. Follow the configuration recommendation in *Table 2-2*.

TABLE 2-2. Upstream Proxy (Dependent) settings in Forward Proxy Mode

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections	8080
Enable upstream proxy (check box)	Enable / Disable upstream proxy	Check (enable)
Proxy Server	IP address of the upstream proxy server	Type in the value of the upstream proxy server
Port	Port of the upstream proxy server	Type in the port number of the upstream proxy server
Enable guest account	Guest mode provides a secondary proxy port that uses the Guest Policy and simplifies deployment without the need to authenticate guests before giving them access to the Internet. In order to enable Internet connectivity to network users who are not in the LDAP directory and apply guest policies, this setting opens a guest port for Web clients to communicate with IWSVA.	Enable and accept the default port of 8081 if you want to support the secondary Guest proxy port. The Guest port can be changed if needed..
Anonymous FTP over HTTP	The email address passed to FTP sites	Change to an appropriate address

4. Click **Next**.
5. Set up the Network Interface on page 2-24 to continue the deployment.

Reverse Proxy Settings

To configure the Proxy Settings for Reverse Proxy Mode:

1. Select the **Reverse Proxy mode** radio button from the Deployment Mode page.

   See Reverse Proxy Mode on page 2-10 for details.
2. Click **Next**.
3. Follow the configuration recommendation in *Table 2-3*/

TABLE 2-3. Reverse Proxy Mode Proxy Settings

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections for reverse proxy.	80
Protected Server	This is the IP address of the Web server IWSVA is protecting.	Type in the IP address of the protected server
Port	This is the SSL port of the Web server IWSVA is protecting.	Type in the SSL port number of the server being protected
Enable SSL Port (check box)	Enable / Disable SSL.	Leave disabled unless required. Check to enable.

4. Click **Next**.
5. Set up the Network Interface on page 2-24 to continue the deployment.

ICAP Settings

Deploying in ICAP Mode requires addition configuration settings.

IWSVA can return four optional headers from the ICAP server whenever a virus is found or information about users and groups. These headers are not returned by default

for performance reasons, because many ICAP clients do not use these headers. They must be enabled in the IWSVA Web console.

- **X-Virus-ID:** Contains one line of US-ASCII text with a name of the virus or risk encountered. For example:

  ```
  X-Virus-ID: EICAR Test String
  ```

- **X-Infection-Found:** Returns a numeric code for the type of infection, the resolution, and the risk description.

  For more details on the parameter values, see:

  `http://www.icap-forum.org/documents/specification/draft-stecher-icap-subid-00.txt`

- **X-Authenticated - User:** If enabled, IWSVA requests the username sent in the X-Authenticated-User ICAP header. The username obtained from the ICAP header allows IWSVA to identify of the user issuing the request if you configure IWSVA to use the user/groupname method of user identification.
- **X-Authenticated - Group:** If enabled, IWSVA requests the group membership information sent in the X-Authenticated-Groups ICAP header if you configure IWSVA to use the user/groupname method of user identification. If disabled, IWSVA queries LDAP for the group membership information.

Note: Some ICAP clients do not offer the recursive group membership search. For example, if a user belongs to group A, and group A belongs to group B, the ICAP client only sends group A information in the header. If you require recursive group membership information, Trend Micro recommends disabling the x_authenticated_groups header.

To configure the ICAP settings:

1. Select the **ICAP mode** radio button from the Deployment Mode page of the Deployment Wizard.

   See ICAP Mode on page 2-11 for details.

2. Click **Next**.
3. Follow the configuration recommendations in *Table 2-4*.

TABLE 2-4. ICAP Mode-specific Settings

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections for ICAP.	1344
Enable X-Virus-ID ICAP header (check box)	Enable / Disable ICAP details about malware detected being recorded.	Enable
Enable X-Infection-Found ICAP header (check box)	Enable / Disable ICAP details about malware detected and passing details back to the ICAP device.	Enable
Enable X-Authenticated-User ICAP header	Enable / Disable ICAP details about username information.	Enable
Enable X-Authenticated-Groups ICAP Header	Enable / Disable ICAP details about group membership information.	Enable

4. Click **Next**.
5. Set up the Network Interface on page 2-24 to continue the deployment.

Note: Complete all steps in the Deployment Wizard to deploy in ICAP mode. After receiving a successful deployment message, configure the IWSVA ICAP set up as shown in *Setting Up IWSVA ICAP* on page 2-41.

Simple Transparency Settings

Simple Transparency Mode requires mode-specific settings.

To configure mode-specific settings for Simple Transparency Mode:

1. Select the **Simple Transparency mode** radio button from the Deployment Mode page.

   See Simple Transparency Mode on page 2-12 for details.
2. Click **Next**.
3. Enter the following settings on the Simple Transparency Settings page. (See *Table 2-5*.)

TABLE 2-5. Simple Transparency Mode-specific Settings

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections.	80
Anonymous FTP over HTTP	The email address passed to FTP sites.	Type in an appropriate email address

4. Click **Next**.
5. Set up the Network Interface on page 2-24 to continue the deployment.

WCCP Settings

WCCP Mode requires mode-specific settings.

To configure mode-specific settings for WCCP Mode:

1. Select the **Web Cache Coordination Protocol (WCCP) mode** radio button from the Deployment Mode page.

   See Web Cache Coordination Protocol (WCCP) Mode on page 2-14 for details.
2. Click **Next**.
3. Enter the following settings on the WCCP Settings page. (See *Table 2-6*.)

TABLE 2-6. WCCP Mode-specific Settings

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections.	80
Router IP address	Detail which router or switch to communicate with via WCCP	Type in the router or switch IP address
Password	Password for WCCP authentication	Type in the password for the WCCP authentication
WCCP forwarding method	The WCCP forwarding method determines how intercepted traffic is transmitted from the WCCP server (IOS) to the WCCP client.	Select the Generic Routing Encapsulation (GRE) or Layer 2 (L2) as the WCCP forwarding method

TABLE 2-6. WCCP Mode-specific Settings (Continued)

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
Note: - GRE forwarding, which is the default forwarding method, encapsulates the intercepted packet in an IP GRE header with a source IP address of the WCCP server (IOS) and a destination IP address of the target WCCP client. This has the effect of a tunnel, allowing the WCCP server (IOS) to be multiple Layer 3 hops away from the WCCP client. - L2 forwarding simply rewrites the destination MAC address of the intercepted packet to equal the MAC address of the target WCCP client. L2 forwarding requires that the WCCP server (IOS) is Layer 2 adjacent to the WCCP client		
Assignment method	WCCP provides packet distribution through two algorithms, Hash tables and Mask/value sets.	Select Hash tables or Mask/value sets as the WCCP assignment method.
With hash assignment, the router runs a value in the header of the packet it is redirecting through a hashing function. With mask assignment, each router/switch in the service group has a table of masks and values that it uses to distribute traffic across the proxy appliances in the service group.		
Anonymous FTP over HTTP	The email address passed to FTP sites.	Type in an appropriate email address

4. Click **Next**.
5. Set up the Network Interface on page 2-24 to continue the deployment.

Network Interface

All modes need the relevant network interface settings configured. Some modes require slightly different information than other modes. The following procedures calls out the different settings needed.

Network interface settings include:

- Host Information on page 2-25
- Data Interface on page 2-28
- Separate Management Interface on page 2-30
- Miscellaneous Settings on page 2-31

Host Information

All modes require the host information to be entered. Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings

To enter the host information:

1. Using the Deployment Wizard, select the appropriate deployment mode radio button and click **Next**.
2. Set any mode-specific settings and click **Next**.
3. Type the applicable Fully Qualified Domain name (FQDN) for the IWSVA host.

> **Note:** A fully qualified hostname is required. Trend Micro recommends creating a DNS entry for the IWSVA server's hostname in their DNS server.

4. Continue to the section about the Interface Status starting on page 2-25.

Interface Status

IWSVA provides a graphical representation of the physical Ethernet ports on the IWSVA server to simplify the configuration of the network ports. The Interface Status graphic shows the status and function of the available interfaces.

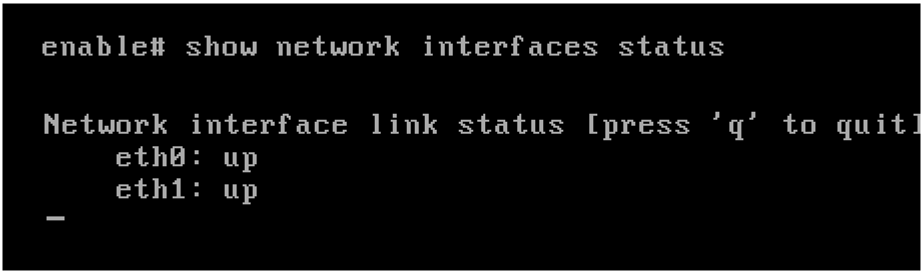
Use *Figure* to interpret the status and function of the Ethernet ports used for configuration purposes in the Interface Status section.

Determining the Status of the Interfaces

IWSVA is a software virtual appliance that can be installed on all types of hardware. As such, the network information displayed in IWSVA's Web UI may not directly relate to the physical network interfaces installed in the server running IWSVA. For example, if the server came with two network interfaces installed on the motherboard and then an additional four-port Ethernet card was installed in the server to increase the network interfaces available, the IWSVA Web UI may display the first network port as Eth0 when it is actually mapped to physical network interface Eth2 on the new Ethernet card.

In order to positively identify the IWSVA Web UI network interface to the physical network interface, IWSVA provides a command line interface (CLI) command to display the real time status of the physical network interfaces and the Interface Status graphic in the Deployment Wizard.

By using the `show network interfaces status` CLI command from the IWSVA console, you can quickly see the link status of the physical interface. In the example below, you can see that Eth0 and Eth1 is up with a physical link connection.



```
enable# show network interfaces status

Network interface link status [press 'q' to quit]
    eth0: up
    eth1: up
_
```

FIGURE 2-9. **"show network interfaces status" CLI command**

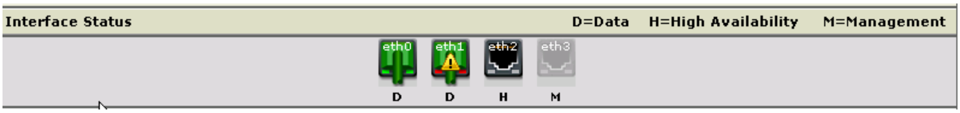
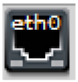
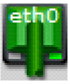
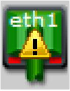
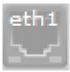


FIGURE 2-10. **Interface Status**

Figure 2-10 depicts the interface status information displays in the Deployment Wizard. *Table 2-2* defines the icons used in the interface status graphic.

TABLE 2-2. Interface Status Icons

CALLOUT	POINTS TO
M	Management interface
D	Data interface
H	HA or Heartbeat Interface
	Link not detected. Could be an empty port, cable may be loose or broken, or the peer machine may be down.
	Link ok
	Link error
	Link disabled

About Interface Mapping

Trend Micro recommends mapping the interfaces with physical interfaces before configuring or modifying your interface settings.

After rebooting IWSVA, the numbering for unused interfaces may change, however the occupied interfaces (for data, management, or HA) will not change.

Before dissolving a cluster, interfaces might be mapped as shown in *Table 2-7*.

TABLE 2-7. Original Interface Mapping

PHYSICAL INTERFACE	A	B	C	D
RELATIVE INTERFACE	eth1	eth2	eth0	eth3
PURPOSE	D (internal	H	D (external)	M

After dissolving a cluster, joining a cluster, or rebooting, the interface mapping might change as shown in *Table 2-8*.

TABLE 2-8. Changed Interface Mapping

PHYSICAL INTERFACE	A	B	C	D
RELATIVE INTERFACE	eth2	eth1	eth0	eth3
PURPOSE	(unused)	(unused)	D (external)	M

Data Interface

The Data Interface supports end-user Internet traffic to and from the internal network. Use the following procedure to configure the host name and IP settings for the data (bridge or proxy) interfaces.

WARNING! **Do NOT configure the data interface and the management interface in the same network subnet. If they are in the same network segment, the IWSVA internal firewall will prevent proper forwarding of HTTP and FTP traffic.**

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the IWSVA host information

To configure the Data Interface settings:

1. Continue working from the **Network Interface** page of the Deployment Wizard.
2. Configure the Data Interface settings:

   a. **All modes except Transparent Bridge mode:** Select the appropriate Ethernet port from the **Ethernet Interface** drop-down list for the data interface.

   The dynamic Interface Status graphic displays your selection.

   b. **Transparent Bridge Mode and Transparent Bridge Mode - High Availability only:** Select the appropriate Ethernet ports from the drop-down lists for the Internal and External interfaces.

   The Interface Status graphic displays your selection.

   c. Select the IP address type from the drop-down list:

   - **Static IP address** - to configure IP settings for the interface manually.
   - **Dynamic IP address (DHCP)** - to have a DHCP server assign IP settings to the interface.

   d. Enter the IP address and Netmask.

   e. Check the **Enable Ping** check box to allow the connection to be checked with the ping utility.

   f. (Optional) **Transparent Bridge Mode and Transparent Bridge Mode - High Availability only:** Click the check box to enable the VLAN ID (1-4094)

   Note: The HA parent unit and the HA child unit have separate, unique VLAN ID settings.

   g. Do one of the following:

   - Continue with the deployment mode settings, if you are setting up IWSVA for the first time or

- Click **Next** and click through the remaining screens if you have already setup your deployment mode and are only modifying the data interface.

3. If needed, set up Data Interface access control list. See Configuring Internet Access Control Settings on page 5-13.
4. Continue to the section about Separate Management Interface starting on page 2-30.

Separate Management Interface

The separate management interface offers administrators an independent interface to log into the IWSVA device, either through the Web console or via SSH.

Enabling and disabling the separate management interface is done by setting the values and enabling them through the Network Settings page of the Deployment Wizard.

Note: The separate management interface must be enabled for HA environments.

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the IWSVA host information
- Configured the Data Interface information

To setup the separate management interface:

1. Continue working from the **Network Interface** page of the Deployment Wizard.
2. Check the check box for the **Enable Management Interface**.
3. Select an **Ethernet interface** from the drop-down list.
4. Enter a **Static IP address** for the management interface device.
5. Enter the **Netmask** for the management interface device.
6. Check the Enable Ping check box to allow the connection to be checked with the ping utility.
7. Do one of the following:
   - Continue with the deployment mode settings, if you are setting up IWSVA for the first time or

- Click **Next** and click through the remaining screens if you have already setup your deployment mode and are just adding the separate management interface.

Miscellaneous Settings

The Miscellaneous Settings section allows you to obtain the dynamic information from DHCP or enter static information for:

- Gateway IP address
- Primary DNS server IP address
- Secondary DNS server IP address

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the IWSVA host information
- Configured data and management interface information

To configure the Miscellaneous settings:

1. Continue working from the **Network Interface** page of the Deployment Wizard.
2. Scroll to the **Miscellaneous Settings** section.
3. Do one of the following:
    - Check the **Obtain from DHCP** check box to have IWSVA obtain the dynamic Gateway, Primary, and Secondary DNS information OR
    - Type in the Gateway, Primary, and Secondary DNS information if it is static.

TABLE 2-9. Miscellaneous Settings information

PARAMETER	DESCRIPTION
Gateway	For static IP address configuration of the network device, type in the applicable IP address used as the gateway for this IWSVA installation.
Primary DNS	For static IP address configuration of the network device, type in the applicable IP address used as the primary DNS server for this IWSVA installation.

TABLE 2-9. Miscellaneous Settings information (Continued)

PARAMETER	DESCRIPTION
Secondary DNS	For static IP address configuration of the network device, type in the applicable IP address used as the secondary DNS server for this IWSVA installation.

4. Click **Next**.
5. Continue to the section on Static Routes starting on page 2-32.

Note: If you are joining an existing cluster, continue with the section on Summary starting on page 2-37.

Static Routes

Static routes allow IWSVA to overcome problems routing traffic to and from network segments beyond the next router hop to which IWSVA connects. Static routes allow you to manually control the router connection used to send traffic to the Internet or back to the end users.

For example, if IWSVA updates patterns with an internal ActiveUpdate (AU) server through a different router, a static route should be added for AU server.

Note: If you bind a static route to an interface, the router port must be in the same network segment as the interface.

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the network interface information

To configure settings for Static Routes:

1. From the Static Routes page in the Deployment Wizard, go to the Settings section and configure the following:
    - Network ID
    - Netmask
    - Router
    - Interface
2. Click **Add to List**.

    The static route displays in the Static Routes list.
3. Add additional static routes.
4. Click **Next**.
5. Continue to Product Activation starting on page 2-33.

Product Activation

After completion of the registration process, performed during deployment, you must activate (or enable) your software. Trend Micro products do not scan traffic or enforce policy settings unless a valid Activation Code is entered.

To receive your Activation Code, you must enter your registration key with the Trend Micro Product Registration server.

About Licenses

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support ("Maintenance") for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis according to Trend Micro's Maintenance Fee pricing.

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement. The Maintenance Agreement expires but your License Agreement will not.

Note: The Maintenance Agreement expires but your License Agreement will not. If the Maintenance Agreement expires, your system will continue scanning, but you will not be able to update the virus pattern file, scan engine, or program files (even manually). Nor will you be entitled to receive technical support from Trend Micro.

Typically, ninety (90) days before the Maintenance Agreement expires, you will start to receive email notifications, alerting you of the upcoming discontinuation. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

`https://olr.trendmicro.com/registration/`

Third-party Licensing Agreements

Access third-party licensing agreements in the following directory:

`/usr/share/doc`

Registering Online

Registration must take place prior to activating the product.

There are several ways to register IWSVA:

- To register if you are a new customer: on page 2-34
- To register if you are a registered user: on page 2-35

To register if you are a new customer:

1. Click the **Trend Micro Product Registration Server** link in your product at **Administration > Product License**.
2. In the Enter Registration Key screen, use the Registration Key that came with your product (Trend Micro Enterprise Protection DVD or License Certificate).
3. Click **Continue**, and then **I CONFIRM**.

   The Confirm Product Information screen appears.
4. Click **Continue with Registration** to confirm all the product information.
5. Next, type all the required contact information in the fields provided and click **Submit**.

6. From the Confirm Registration Information screen, click **Edit** to update your contact information and click **OK** to continue.

   The Activation Code screen appears. Your Activation Code will be sent to your registered email address.

7. Click **OK** to finish.

To register if you are a registered user:

1. Click the **Trend Micro Product Registration Server** link in your product at **Administration > Product License**.
2. Type your Logon ID and password in the fields provided, and then click **Login**.

   You will be prompted to change your password the first time you log on.

3. In the My Products screen, click **Add Products** and type the Registration Key.
4. To edit your company profile, click **View/Edit Company Profile.**

   Your Activation Code appears on the next screen.

5. To receive a copy of your Activation Code at your registered email address, click **Send Now**.

Note: For maintenance renewal, contact Trend Micro sales or your reseller. Click Check Status Online at Administration > Product License to update the maintenance expiration date on the Product License screen manually.

About Activation Codes

An Activation Code is required to enable scanning and product updates. You can activate IWSVA during Setup or anytime thereafter. Register IWSVA during installation to receive an Activation Code.

Note: After registering IWSVA, you will receive an Activation Code via email. An Activation Code has 37 characters (including the hyphens) and looks like:

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

A Registration Key has 22 characters (including the hyphens) and looks like:

```
xx-xxxx-xxxx-xxxx-xxxx
```

- You automatically receive an evaluation Activation Code if you download IWSVA from the Trend Micro Web site
- You can use a Registration Key to obtain an Activation Code online

You can find an evaluation Registration Key on the Trend Micro Enterprise Protection DVD. Use this key to obtain an Activation Code. You will get an evaluation Activation Code by email when you download IWSVA from the Web.

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the network interface information
- Configured the static routes

To activate IWSVA:

1. Go to the **Product Activation** page in the Deployment Wizard.
2. Type the **Activation Code** for IWSVA.
3. Click **Next**.
4. Continue with System Time Settings starting on page 2-36.

System Time Settings

System Time and Time Zone settings allow you to:

- Use the current system time
- Synchronize with your NTP server
- Enter the date and time manually
- Select your time zone

Before starting this procedure, be sure you have:

- Selected your deployment mode
- Configured any mode-specific settings
- Configured the network interface information
- Configured the static routes
- Entered product activation information

To set the system time and time zone settings:

1. Access the System Time page of the Deployment Wizard.
2. Select from one of the following options:
   - Current system time - keep the time already set on the system
   - Synchronize with NTP server -
   - Manually - Set the date and time manually
3. Set the appropriate time zone.
   - Select your continent from the drop-down list.
   - Select your city (or a city near you with the same time as your location) from the drop-down list.
4. Click **Next.**
5. Continue with Summary on page 2-37.

Summary

The Summary page displays your IWSVA configuration settings so you can verify them. If you seen an error, click the Back button and return to appropriate page. You can return to this page any time you need to view a summary of your settings.

To submit your deployment mode information.

1. Access the Summary page of the Deployment Wizard.
2. Review the following settings:
   - Host name
   - HTTP Listening port number
   - Anonymous FTP over HTTP contact email address
   - HA Interface (High Availability mode only)
   - Data Interface settings
   - Management Interface settings
   - Miscellaneous settings
   - Static Route Settings
   - Product Activation
   - System Time Settings

3. If your settings are incorrect, click **Back** and correct the information on the appropriate screen.
4. If your settings are correct, click the **Submit** button.

   Clicking Submit saves your settings. These settings can be edited after the results display by accessing Administration > Deployment Wizard.
5. Continue with the section about Results starting on page 2-38.

Results

The results page will let you know if your settings were entered successfully and that IWSVA has been deployed. It will also indicate if your settings were not accepted.

The system checks deployment settings at the time of entry, before you move from one page in the Deployment Wizard to the next. Successful results are the most common outcome.

Deployment Status

This messages displays if your IWSVA deployment was successful with a status bar that reflects the on-going deployment your mode settings.

> "Congratulations! Your appliance has been set up and deployed."
>
> You will be redirected to <IWSVA Web Console IP address> shortly. It may take several minutes for the system to implement the new configuration changes and to restart before allowing you to log in."

Note: Trend Micro recommends you update IWSVA as soon as you receive this message. For more information, see Chapter 4, *Updates* starting on page 4-1.

If your deployment is successful, you could receive a message indicating a problem accessing the Web console. The message contains a suggestion on how to fix the problem. See the sample below.

> "You designated DHCP protocol to configure the IWSVA network interface, which prohibits the Deployment Wizard from finding the Web console IP address automatically. The IP address and port number can be obtained from the IWSVA server display."

Post Deployment

After the Deployment Wizard is successfully configured, IWSVA will automatically reboot.

After IWSVA reboots, Trend Micro recommends you update IWSVA as soon as possible. See Updates on page 4-1 for details.

Also:

- If you deployed in Transparent Bridge mode, see LAN-bypass Function on page 2-39 for details on failopen NIC support.
- If you deployed in ICAP mode, see Setting Up IWSVA ICAP on page 2-41 for details on setting up an ICAP-compliant cache server to work with IWSVA.
- See Testing and Configuring IWSVA on page 14-1 for step-by-step processes to validate your installation.

LAN-bypass Function

The LAN-bypass function allows the customer to install a Trend Micro supported fiber or Gigabit network interface card (NIC) into the supported server platform to allow the network traffic to be by-passed on specific error conditions.

Note: IWSVA only supports LAN-bypass functionality in Transparent Bridge Mode.

Setup the by-pass function in one of three settings:

- **Auto**—Bypass is OFF when the system is in a normal state; Bypass mode is ON when system detects an abnormal state such as kernel panic issue or when power is cut off from the IWSVA unit
- **On**—Always bypass traffic
- **Off**—Never bypass traffic

Note: When the LAN-bypass function is set to ON, the data interface is not available. However, the customer can still access IWSVA via the separate management interface, if configured.

The LAN-bypass function supports two port Silicom cards:

- **SD:** PXG2BPFIL-SD, PXG2BPI-SD
- **Non-SD:** PEG2BPFID, PEG2BPI

Enabling the LAN-bypass Function

The following procedure allows you to change the default settings for the LAN-bypass feature. Examples of when to change the parameters can include:

- Installing a new LAN-bypass card
- Selecting NICs supporting LAN bypass for the data interface
- Changing the default LAN-bypass mode

If you select one of the supported NICs that can perform hardware bypass in the Deployment Wizard, it will be enabled with the AUTO setting. Under the AUTO setting, the IWSVA monitors the critical services and OS kernel for crashes. If it detects an unrecoverable error, it will open the NIC into "fail open" or bypass mode.

Use the `show network lanbypass` command to check LAN bypass status on IWSVA.

To display/enable/disable/change the LAN-bypass service on the IWSVA unit:

1. Login to the CLI interface.
2. Execute one of the following commands in *Table 2-10*.

TABLE 2-10. LAN-bypass CLI Commands

COMMAND	DESCRIPTION
`show network lanbypass`	Displays the current configuration status of LAN-bypass function.
`configure network lanbypass on`	Always bypasses traffic. After running this command, all traffic will be bypassed by LAN-bypass card. Administrators may not be able to access the IWSVA device from the network data interface. The system will not adjust the LAN bypass status at any time.

TABLE 2-10. LAN-bypass CLI Commands (Continued)

COMMAND	DESCRIPTION
`configure network lanbypass off`	Never bypasses traffic. The system will not adjust the LAN bypass status at any time.
`configure network lanbypass auto`	The system will auto-adjust the LAN bypass status. For example, when system starts and stops, the bypass will be turned off and turned on. When system is in an abnormal state (such as kernel panic), the bypass will be turned on. After recovery, the bypass will be turned off automatically.

The LAN bypass card configuration is saved at: /etc/lanbypass.conf. Migration updates the mapping table to import or export the LAN bypass configuration.

Setting Up IWSVA ICAP

Perform these configuration steps if you are running IWSVA with an ICAP handler.

1. Setting up an ICAP 1.0-compliant Cache Server on page 2-41
2. Flushing Existing Cached Content from the Appliance on page 2-49

Note: The ICAP setup procedures below apply to the ICAP versions listed under X-Authenticated ICAP Headers Support on page 1-5. They are provided for your convenience; consult the native documentation for complete information.

Setting up an ICAP 1.0-compliant Cache Server

Configure an ICAP client (Network Appliance NetCache appliance/Blue Coat Port 80 Security Appliance cache server/Cisco ICAP server) to communicate with the ICAP server.

See the appropriate process for your ICAP client:

- To set up ICAP for NetCache Appliance: on page 2-42
- To set up ICAP for the Blue Coat Port 80 Security Appliance: on page 2-44

- To set up Cisco CE ICAP servers: on page 2-46

To set up ICAP for NetCache Appliance:

1. Log onto the NetCache console by opening `http://{SERVER-IP}:3132` in a browser window.
2. Click the **Setup** tab, then click **ICAP** > **ICAP 1.0** on the left menu.
3. Click the **General** tab, then select **Enable ICAP Version 1.0**.
4. Click **Commit Changes**.

Note: An error message "`icap: This service is not licensed.`" appears if you have not provided the required ICAP license key for NetCache.

5. Enter an ICAP license key:
   a. Click the **Setup** tab, and then click **System > Licenses** in the left menu. The **System Licenses** screen opens.
   b. Type your license under the **ICAP license** section.
   c. Click **Commit Changes**.
6. Select the **Service Farms** tab on the **ICAP 1.0** screen, then click **New Service Farm** to add ICAP servers. Assign the service farm name in the **Service Farm Name** field.
   - For response mode, select **RESPMOD_PRECACHE** in the **Vectoring Point** field.
   - For request mode, select **REQMOD_PRECACHE** in the **Vectoring Point** field.
7. Select **Service Farm Enable**.
8. In the **Load Balancing** field, choose the proper algorithm to use for load balancing (if you have more than one ICAP server in the service farm). Clear **Bypass on Failure**.

Note: Disable **Bypass on Failure** if your priority is to limit virus propagation within your network. Otherwise, enable **Bypass on Failure** to guarantee an unblocked connection to the Internet.

9. Under the **Consistency** field, choose **strong** from the drop-down menu and leave the **lbw Threshold** field empty.

> **Note:** For multiple ICAP servers within a service farm with **strong** consistency selected, make sure that all ICAP servers have identical `intscan.ini` and other configuration files and the same virus pattern. The service farm will not work properly if the ICAP servers have different configurations.

10. Under the **Services** text box (for response mode), type:

    ```
    icap://{ICAP-SERVER-IP}:1344/RESP-Service on
    ```

    where `ICAP-SERVER-IP` is the IP address of IWSVA ICAP for response mode.

    a. For multiple IWSVA ICAP server services, type the additional entries for response mode:

    ```
    icap://{ICAP-SERVER1-IP}:1344/resp on
    icap://{ICAP-SERVER2-IP}:1344/resp on
    ```

11. Under the **Services** text box (for request mode), type

    ```
    icap://{ICAP-SERVER-IP}:1344/REQ-Service on
    ```

    where `ICAP-SERVER-IP` is the IP address of IWSVA ICAP for request mode.

    a. For multiple IWSVA ICAP server services, type the additional entries for request mode:

    ```
    icap://{ICAP-SERVER1-IP}:1344/REQ-Service on
    icap://{ICAP-SERVER2-IP}:1344/REQ-Service on
    ```

12. Click **Commit Changes**.
13. Click the **Access Control Lists** tab, then select **Enable Access Control Lists**.
14. Type "`icap (Service Farm name of the ICAP Server) any`" in **HTTP ACL.**
15. Click **Commit Changes**.
16. To configure scanning FTP over HTTP traffic, go to **Access Control List** and add "icap (service farm name)" into the **FTP ACL** field.

To set up ICAP for the Blue Coat Port 80 Security Appliance:

1. Log onto the Web console by typing `https://{SERVER-IP}:8082` in the address bar of your Web browser.

Note: The procedure for setting up ICAP on a Blue Coat appliance might vary depending on the product version.

2. Select **Management**.
3. Type the logon user name and password, if prompted.
4. Click **ICAP** in the left menu, then click the **ICAP Services** tab.
5. Click **New**.

   The **Add ICAP Service** screen opens.
6. In the **ICAP service name** field, type an alphanumeric name. Click **Ok**.
7. Highlight the new ICAP service name and click **Edit**.

   The **Edit ICAP Service name** screen opens.
8. Type or select the following information:

   a. The ICAP version number (that is, 1.0)

   b. The service URL, which includes the virus-scanning server host name or IP address, and the ICAP port number. The default ICAP port number is 1344.

   - Response mode:

   ```
   icap://{ICAP-SERVER-IP}:1344
   ```

   - Request mode:

   ```
   icap://{ICAP-SERVER-IP}:1344/REQ-Service
   ```

   where `ICAP-SERVER-IP` is the IP address of IWSVA ICAP.

   c. The maximum number of connections (ranges from 1-65535). The default value is 5.

   d. The connection time-out, which is the number of seconds the Blue Coat Port 80 Security Appliance waits for replies from the virus-scanning server. The range is an interval from 60 to 65535. The default time-out is 70 seconds.

   e. Choose the type of method supported (response or request modes).

   f. Use the default preview size (bytes) of zero (0).

g. Click **Sense settings** to retrieve settings from the ICAP server (recommended).

h. To register the ICAP service for health checks, click **Register** under the **Health Check Options** section.

9. Click **Ok**, then click **Apply**.

Note: You can edit the configured ICAP services. To edit a server configuration again, select the service and click **Edit**.

10. Add the response or request mode policy.

    The Visual Policy Manager requires the Java 2 Runtime Environment Standard Edition v.1.3.1 or later (also known as the Java Runtime or JRE) from Sun™ Microsystems, Inc. If you already have JRE on your workstation, the Security Gateway opens a separate browser window and starts the Visual Policy Manager. The first time you start the policy editor, it displays an empty policy.

    If you do not have JRE on your workstation, a security warning window opens. Click **Yes** to continue. Follow the instructions.

To add the response mode policy:

1. Select **Management**.

   Type the logon user name and password if prompted.

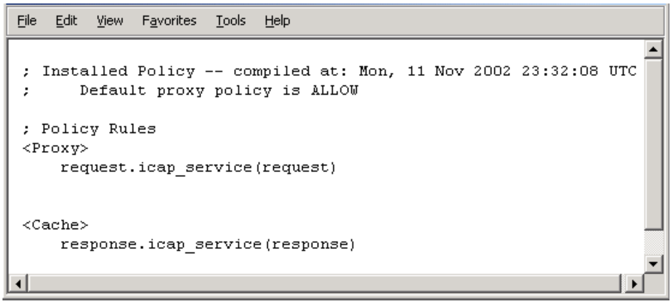
2. Click **Policy** on the left menu, then click the **Visual Policy Manager** tab.
3. Click **Start**. If the **Java Plug-in Security Warning** screen appears, click **Grant this session**.
4. On the menu bar, click **Edit > Add Web Content Policy**. The **Add New Policy Table** screen opens.
5. Type the policy name under the **Select policy table name** field. Click **OK**.
6. Under the **Action** column, right-click **Bypass ICAP Response Service** and click **Set**. The **Add Object** screen opens. Click **New** and select **Use ICAP Response Service**. The **Add ICAP Service Action** screen opens.
7. Choose the ICAP service name under the **ICAP Service/Cluster Names** field. Enable **Deny the request** under the **On communication error with ICAP service** section. Click **OK**, then click **OK** again.

8. Click **Install Policies**.

To add the request mode policy:

1. Follow Step 1 through Step 5 in the previous procedure.
2. Under the **Action** column, right-click **Deny** and click **Set**. The **Add Object** screen opens. Click **New** and select **Use ICAP Request Service**. The **Add ICAP Service Action** screen opens.
3. Choose the ICAP service name under the **ICAP Service/Cluster Names** field.
4. Enable **Deny the request** under the **On communication error with ICAP service** section.
5. Click **OK** and then **OK** again.
6. Click **Install Policies**.
7. Configure both the request and response mode ICAP services.

   To check the current policy, go to the Policy screen, click the **Policy Files** tab, and then click **Current Policy**.



```
; Installed Policy -- compiled at: Mon, 11 Nov 2002 23:32:08 UTC
;     Default proxy policy is ALLOW

; Policy Rules
<Proxy>
    request.icap_service(request)


<Cache>
    response.icap_service(response)
```

FIGURE 2-11. Install Policies screen

To set up Cisco CE ICAP servers:

IWSVA supports Cisco ICAP servers (CE version 5.1.3, b15). All ICAP settings are performed through a command line interface (CLI); there is no user interface associated with the Cisco ICAP implementation.

1. Open the Cisco CE console.
2. Type **`config`** to enter the configuration mode.
3. Type **`icap?`** to display a list of all ICAP-related commands.

4. Create a response modification service, by typing:

   ```
   icap service RESPMOD SERVICE NAME
   ```

   This takes you into the ICAP service configuration menu. Type **`?`** to display a list of all available commands. Type the following commands:

   `server icap://ICAP SERVER IP:1344/resp` (to assign a server type)

   `vector-point respmod-precache` (to assign the proper vector point type)

   `error-handling return-error` (to assign the proper error-handling type)

   `enable` (to enable the ICAP multiple server configuration)

5. Type **`exit`**.
6. Create a request modification service, by typing

   ```
   icap service REQUESTMOD SERVICE NAME
   ```

   This command takes you into the ICAP service configuration menu. Type **`?`** to display a list of all available commands. Issue the following commands:

   `server icap://ICAP SERVER IP:1344/REQ-Service` (to assign a server type)

   `vector-point reqmod-precache` (to assign the proper vector point type)

   `error-handling return-error` (to assign the proper error-handling type)

   `enable` (to enable the ICAP multiple server configuration)

7. Type **`exit`**.
8. For additional configuration steps, type the following:

   `icap append-x-headers x-client-ip` (to enable X-client headers for reports)

   `icap append-x-headers x-server-ip` (to enable X-server headers for reports)

   `icap rescan-cache ISTag-change` (to turn on ISTAG rescan for updates)

   `icap bypass streaming-media` (to exclude streaming media from ICAP scanning)

   `icap apply all` (to apply all settings and activate ICAP type)

   `show icap` (to display current ICAP configuration at root CLI menu)

Configuring Virus-scanning Server Clusters

For the Blue Coat Port 80 Security Appliance to work with multiple virus-scanning servers, configure a cluster in the Security Gateway (add the cluster, and then add the relevant ICAP services to the cluster).

To configure a cluster using the Web console:

1. Select **Management**.

   Type the logon user name and password if prompted.

2. Click **ICAP** on the left menu, then click the **ICAP Clusters** tab.
3. Click **New**.

   The **Add ICAP Cluster** screen opens.

4. In the **ICAP cluster name** field, type an alphanumeric name and click **Ok**.
5. Highlight the new ICAP cluster name and click **Edit**.

   The **Edit ICAP Cluster name** screen opens.

6. Click **New** to add an ICAP service to the cluster.

   The **Add ICAP Cluster Entry** screen opens. The pick list contains a list of any services available to add to the cluster. Choose a service and click **Ok**.

7. Highlight the ICAP cluster entry and click **Edit**.

   The **Edit ICAP Cluster Entry name** screen opens. In the **ICAP cluster entry weight** field, assign a weight from 0-255. Click **Ok**, click **Ok** again, and then click **Apply**.

Deleting a Cluster Configuration or Entry

You can delete the configuration for an entire virus-scanning server cluster, or you can delete individual entries from a cluster.

Note: Do not delete a cluster used in a Blue Coat Port 80 Security Appliance policy if a policy rule uses a cluster name.

To delete a cluster configuration using the Web console:

1. Select **Management**.

   Type the logon user name and password if prompted.

2. Click **ICAP** on the left menu, then click the **ICAP Clusters** tab.
3. Click the cluster you want to delete. Click **Delete**, then click **Ok** to confirm.

Flushing Existing Cached Content from the Appliance

There is a potential risk of infection from content cached to the NetCache appliance, Blue Coat Port 80 Security Appliance, or the Cisco ICAP servers before IWSVA ICAP started scanning HTTP traffic. To safeguard against this possibility, Trend Micro recommends flushing the cache immediately after configuring IWSVA ICAP. All new requests for Web content are then served from the Internet and scanned by IWSVA ICAP before caching. Scanned content is then cached on the NetCache appliance, Blue Coat Port 80 Security Appliance, or the Cisco ICAP servers. The NetCache appliance, the Blue Coat Port 80 Security Appliance, or the Cisco ICAP servers serve future requests for the same Web content by your network users. Because the request is not sent to the Internet, download time is accelerated.

To flush the cache in NetCache:

1. Click the **Utilities** tab, then click **Cache Objects** on the left menu.
2. Click **Flush** under the **Flush the Cache** section.

To flush the cache in the Blue Coat Port 80 Security Appliance:

1. Select **Management**.

   Type the logon user name and password if prompted.
2. Click **Maintenance**.
3. Click the **Tasks** tab and click **Clear**. Click **OK** to confirm.

To flush the cache in the Cisco ICAP server:

1. Telnet to Cisco CE.
2. At the root CLI menu, type **cache clear**.
3. Press **Enter**.

Verifying that InterScan Web Security Virtual Appliance is Listening for ICAP Requests

To verify that IWSVA is listening on the correct port, use PuTTY to access IWSVA via SSH as the “admin” user.

Once logged in as the "admin" user, issue the CLI command `show network connections all` to show all active network connections through IWSVA. There should now be a TCP port access available on port **1344**.

Sample of command and output:

```
enable# show network connections all
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
State
tcp        0      0 0.0.0.0:9091                0.0.0.0:* LISTEN
tcp        0      0 127.0.0.1:8005              0.0.0.0:* LISTEN
tcp        0      0 0.0.0.0:1812                0.0.0.0:* LISTEN
tcp        0      0 0.0.0.0:22                  0.0.0.0:* LISTEN
tcp        0      0 0.0.0.0:5432                0.0.0.0:* LISTEN
tcp        0      0 10.204.170.156:22             10.204.170.158:2665
ESTABLISHED
udp         0      0 0.0.0.0:514                  0.0.0.0:*
udp         0      0 0.0.0.0:21273                0.0.0.0:*
udp         0      0 0.0.0.0:35739                0.0.0.0:*
udp         0      0 0.0.0.0:7068                 0.0.0.0:*
udp         0      0 0.0.0.0:17437                0.0.0.0:*
udp         0      0 0.0.0.0:22688                0.0.0.0:*
udp         0      0 0.0.0.0:9911                 0.0.0.0:*
udp         0      0 0.0.0.0:30138                0.0.0.0:*
udp         0      0 0.0.0.0:60733                0.0.0.0:*
udp      0     0 127.0.0.1:9925           127.0.0.1:9925
ESTABLISHED
udp         0      0 0.0.0.0:36946                0.0.0.0:*
udp         0      0 0.0.0.0:41560                0.0.0.0:*
udp         0      0 0.0.0.0:29294                0.0.0.0:*
udp         0      0 0.0.0.0:12655                0.0.0.0:*
udp         0      0 0.0.0.0:38390                0.0.0.0:*
udp         0      0 0.0.0.0:7036                 0.0.0.0:*

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State     I-Node    Path
unix  2   [ ACC ] STREAM  LISTENING 6643358 /tmp/ssh-ddgvf12499/agent.12499
unix  2   [ ACC ] STREAM  LISTENING 634599   /var/run/nscd/socket
unix  2   [ ACC ]  STREAM LISTENING   7249   /var/run/dbus/system_bus_socket
unix  2   [ ACC ]  STREAM LISTENING   7368   @/var/run/hald/dbus-uIGJbIMMam
unix  2[ ]        DGRAM              6421523 /tmp/tmsyslog
unix  2    [ ]     DGRAM              6421525 /tmp/log
unix  2    [ ACC ] STREAM LISTENING   3065236/tmp/.s.PGSQL.5432
unix  2    [ ]     DGRAM              1274   @/org/kernel/udev/udevd
unix  2    [ ]     DGRAM              7379 @/org/freedesktop/hal/udev_event
unix  2    [ ACC ] STREAM LISTENING   7369 @/var/run/hald/dbus-0oDgnh6zwa
unix  5    [ ]     DGRAM              6430159 /dev/log
unix  2    [ ]     DGRAM              6643350
unix  2    [ ]     DGRAM              6603791
unix  2    [ ]     DGRAM              6430163
unix  2    [ ]     DGRAM              065234
unix  3    [ ]     STREAM CONNECTED   8017 /var/run/dbus/system_bus_socket
unix  3    [ ]     STREAM CONNECTED   8016
unix  3    [ ]     STREAM CONNECTED   8003 @/var/run/hald/dbus-uIGJbIMMam
unix  3    [ ]     STREAM CONNECTED   8002
unix  3    [ ]     STREAM CONNECTED   7872 @/var/run/hald/dbus-uIGJbIMMam
unix  3    [ ]     STREAM CONNECTED   7870
unix  3    [ ]     STREAM CONNECTED   7835 @/var/run/hald/dbus-uIGJbIMMam
unix  3    [ ]     STREAM CONNECTED   7834
unix  3    [ ]     STREAM CONNECTED   7372 @/var/run/hald/dbus-0oDgnh6zwa
unix  3    [ ]     STREAM CONNECTED   7371
unix  3    [ ]     STREAM CONNECTED   7257
unix  3    [ ]     STREAM CONNECTED   7256
    enable#
```

Understanding the Differences between Request Mode and Response Mode

ICAP Request Mode: When a new request is received, the request is sent to the scanning server to ensure it is a valid access request.

ICAP Response Mode: When the new request is valid, any returned content is scanned.

It is possible to use only one scanning vector; however, this reduces the ability to scan all appropriate traffic by 50%.

Triggering a Request Mode Action

The steps outlined below are specifically for the triggering of a request mode action through InterScan Web Security Virtual Appliance which further triggers a Damage Cleanup Services (DCS) attempt (If a DCS server is used and IWSVA has registered to the DCS server successfully):

1. Log into the Windows XP Service Pack 3 client as one of the user accounts created on the Active Directory domain.
2. Open a Web browser and open the site www.goodclup.com/caiink/t1.exe

The outbound URL is passed to InterScan Web Security Suite and is blocked. If a DCS server is used and IWSVA has registered to the DCS server successfully, as Damage Cleanup Services is still configured to perform an automatic cleanup, the workstation also has an automatic remediation attempt performed against it.

Triggering a Response Mode Action

The steps outlined below are specifically for the triggering of a response mode action through IWSVA.

1. Login to the Windows XP Service Pack 3 client as one of the user accounts created on the Active Directory domain.
2. Open a Web browser and open the site www.eicar.org.
3. Click on the button labeled **AntiMalware Testfile**.
4. Scroll to the bottom of the page where it details **Download area using the standard protocol http.**
5. Select the **eicar.com.txt** file to download.

The outbound URL is valid, thus the request mode allowed the URL to pass. The response of the traffic — the actual download triggers InterScan Web Security to block the download from occurring.

Chapter 3

High Availability and Cluster Management

This chapter discusses how High Availability functions and how to use the Cluster Management interface.

Topics in this chapter include the following:

High Availability Overview

IWSVA provides High Availability (HA) to ensure business continuity using active/passive pairs deployed in Transparent Bridge mode.

Note: The IWSVA HA solution currently only supports active/passive pairs in “Transparent Bridge mode for High Availability.” It only supports two HA nodes in one HA cluster.

The four terms to describe HA cluster members are:

- **Active member**—The IWSVA unit providing real-time content scanning.
- **Passive member**—The IWSVA unit in passive standby mode.
- **Parent member**—The IWSVA unit responsible for accepting all configuration changes and synchronizing the policy and configuration with the child member.
- **Child member**—The IWSVA unit that is receiving the policy and configuration changes in the background.

HA switchover can be automatic (failover) or manual.

For failover:

- IWSVA's HA service monitors the critical services of the IWSVA application and the underlying OS for failures. If an abnormality occurs on the active unit, the HA service switches from the active node to the passive node automatically.
- Some of the administrator's HA management operations—like joining of a node or the shutdown of the parent—can trigger an automatic switchover. HA handles this type of switchover gracefully and automatically.

For manual switchover:

- Administrators can manually force an HA switch over using the Web console on the parent node.

Note: 1) HA disables the LAN By-pass feature. It is not required with HA.
2) HA requires the enabling of the Spanning Tree Protocol (STP). This prevents the creation of Layer 2 loops in the network.
3) If the switch used by the HA solution supports Rapid Spanning Tree Protocol (RSTP), then this requires that STP be disabled on the IWSVA to provide faster switching.
4) Enabling STP/RSTP requires disabling the PortFast Bridge Protocol Data Unit (BPDU) guard on both switches because BPDU disables the ports on the switches and prevents HA from functioning.

About Active/Passive Pairs

The active/passive pair can be connected directly together or through a dedicated switch. The active/passive pair requires two private IP addresses and a private reserved subnet for proper configuration. These private IP addresses are reserved for the HA function's internal use and are used for HA heartbeat information and data synchronization. No user devices are allowed on this private subnet.

IWSVA uses a cluster IP address for the active/passive pair, which is used for managing the HA cluster. This cluster management IP address floats between the two HA units and is always associated with the active member of the HA pair.

The active node scans HTTP, HTTPS, and FTP traffic. The passive node works as stand-by device which does not scan traffic in normal conditions. The passive node can become the active node if an abnormal condition occurs in the active node, such as:

- Data link failure
- OS kernel panic
- Critical services of the IWSVA application fail

IWSVA triggers a failover when the active unit goes down, whether it is caused by a heartbeat down, application down, or system down condition. When a failed unit is brought back online, a user-defined policy determines which unit becomes the newly elected active unit. Administrators can configure the election policy to allow the passive unit to remain as the active unit (normal mode), or configure the election policy with node weighting to always allow a specific HA member to regain control as the active unit.

The HA Agent Handles Status Changes

The IWSVA device that joins the cluster as the first member becomes the active parent node by default.

If the Weighted Priority Election feature is not enabled, the second IWSVA device that joins an existing cluster becomes the passive child node by default.

If the Weighted Priority Election feature is enabled, and a second IWSVA device joins an existing cluster with a higher weighting than the first cluster member, that higher weighted, second machine becomes the active parent member and the original member becomes the passive child member.

Failover vs. Switchover

Failover occurs when the active node crashes or fails to handle traffic normally. IWSVA automatically switches over to the passive standby machine in the cluster and elects the new machine to be the active member.

Switchover occurs when a manual role change is forced through the parent's web management interface—allowing the original child/passive unit to become the new parent/active unit.

HA Agent and Interfaces

The HA Agent can be configured with the following management features:

- About the Deployment Wizard on page 3-4
- About the Application Health Monitor on page 3-5
- About Central Management on page 3-6
- About Cluster Management on page 3-10

About the Deployment Wizard

Use the Deployment Wizard to access the following operations:

- Creating a Cluster on page 3-5
- Joining a Cluster on page 3-5

Note: For more about using the Deployment Wizard, see Chapter 2, *Deployment Wizard*..

Creating a Cluster

A new HA cluster is created through the Deployment Wizard interface. When a new HA cluster is created, the management system configures the HA Agent with the desired policy settings and stores it on the parent member. Parent members are the only units that can be actively configured. A child member receives regular updates from the parent member to stay synchronized with the latest configuration and policy information. See step-by-step instructions for creating a cluster at Create a New Cluster on page 2-6.

Joining a Cluster

When HA members are added to the HA cluster, the Deployment Wizard captures and configures each member with the appropriate network and weight information to setup the parent and child members.

The member with the higher weighting becomes the parent member. This allows you to manually elect the machine that will become the primary active unit.

The HA Agent is responsible for synchronizing the information between the cluster members and for initiating the failover or switchover.

See step-by-step details at Join an Existing Cluster on page 2-7.

About the Application Health Monitor

The Application Health Monitor is a separate service that monitors the IWSVA application and operating system health. It also communicates all necessary information with the HA Agent to allow rapid failover between the active and passive members.

Link Loss Detection

The parent node monitors the Layer 2 switch connection for failures. If network connectivity is lost on the data port, a switchover is automatically generated to allow a rapid failover to the passive standby member.

The `linkloss_timeout` parameter controls the amount of downtime for the link loss detection. When the timer value set in the linkloss_timeout parameter is reached, the failover process is initiated.

The Health Monitor configuration file allows you to configure the `linkloss_timeout` value. The default is 10 seconds. It is located at in the Health Monitor configuration file at: `/etc/iscan/intscan.ini`.

```
[monitor]

linkloss_timeout=10
```

About Central Management

The Central Management is feature is used to manage the two HA nodes as a single device. This allows configuration changes to take place on the parent unit and be automatically synchronized with the child unit.

Note: Central Management only applies to the active/passive pair scenario. It cannot be used for single devices.

The Central Management automatically synchronizes configuration information between the parent and child members every five minutes. Administrators can also manually trigger synchronization by clicking the "Synchronize Now" button on the title bar of the IWSVA Web console Summary page accessed through the parent node.

IWSVA supports two synchronization mechanisms:

- **Automatic synchronization**—The parent node runs a scheduled task every five minutes to synchronize policies and configurations to the child node.
- **Manual synchronization**—Users can force a synchronization by clicking **Synchronize Now** on the **Administration > IWSVA Configuration > Summary** page of the Web console of the parent node.

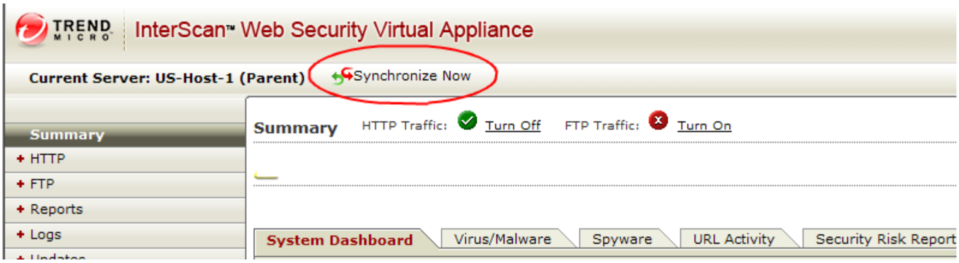


FIGURE 3-1. Synchronization button displays when logged into the parent node.

Users cannot perform a manual switchover if the configurations on the two nodes are not synchronized. If the configurations are not synchronized during a switchover attempt, IWSVA displays a warning message instructing you to manually synchronize the two members first.

For automatic failovers, the switchover happens immediately without a forced synchronization, and any configuration changes made since the last completed synchronization are lost.

Synchronizing Nodes Manually

Synchronization from the parent member to the child member occurs every five minutes. Administrators can manually trigger an immediate synchronization between the cluster members from the Cluster Management page.

To manually synchronize two nodes:

1. Go to the **Summary** page in the parent member Web console.
2. Click **Synchronize Now** at the top of the Summary page. (See *Figure 3-1*.)
3. Click **OK** in the confirmation to immediately synchronize your policies and deployment settings from the parent member to the child member.

Centrally Managed and Non-centrally Managed Features

Some features may be managed centrally, while others require administrators to log into the Web console of the parent or child node. See *Table 3-1* for details.

TABLE 3-1. Centrally Managed vs. Non-centrally Managed Features

CLUSTER-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT NODE	INSTANCE-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT OR CHILD NODE
Enable/disable HTTP(S)/FTP traffic (on Summary page)	Summary • System Dashboard /Virus/Malware/URL/Spyware/ Security Risk Report
All HTTP(s) policies and settings (under HTTP(S) section) • Includes HTTPS certifications	Reports (features and data) • Real-time reports • Scheduled reports data
All FTP policies and settings (under FTP section)	Logs (features and data) • Log query • Log deletion
Report Settings • Scheduled Report Settings • Report Templates • Configuration	Updates (manual update)
Log Settings • Syslog Configuration • Log Settings	Test database connection feature (under Administration > IWSVA Configuration > Database Connection)

TABLE 3-1. Centrally Managed vs. Non-centrally Managed Features (Continued)

CLUSTER-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT NODE	INSTANCE-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT OR CHILD NODE
Update Settings • Scheduled Update Settings • Connection Settings	Interface Configuration for data port and management port • Hostname • IP address and net mask • Port for data interface or management interface
Notification settings • Notification page • Threshold Alert Settings on Summary page • SMTP settings • SNMP settings under Administration > Network Configuration > SNMP Settings	TMCM Registration
Policy deployment settings (under Administration > Policy Deployment)	DCS Registration
Quarantine Management (under Administration > Quarantine Management)	System patch
System Time	Update OS
Network Settings (Except Hostname, IP, net mask, and port) • Enable Ping for each interface • DNS • Default Gateway • Static Routes **Note:** DHCP is removed in HA	Support

TABLE 3-1. Centrally Managed vs. Non-centrally Managed Features (Continued)

CLUSTER-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT NODE	INSTANCE-LEVEL SETTINGS AVAILABLE THROUGH THE PARENT OR CHILD NODE
Web Console settings (under Administration > Network Configuration > Web Console)	
Remote CLI settings (under Administration > Network Configuration > Remote CLI)	
User accounts (under Administration)	
Configuration backup/restore	
Product License	
DEPLOYMENT WIZARD CONFIGURATIONS	
System time Deployment Mode Static Routes Data Interface & Management Interface • DNS • Default gateway • Static Router • Enable PING	Data Interface and Management Interface • Hostname • IP address and net mask • Port number

About Cluster Management

The Cluster Management screen is located at **Administration > IWSVA Configuration > Cluster Management** and is used to configure the HA cluster. The cluster settings are saved in the cluster configuration file and used by the Central Management feature and the HA Agent to create the HA policies and failover priorities.

Changing the weight values of the cluster members allow manual parent/active member selection, but may also cause a switchover to occur. See About Weighted Priority Election on page 2-6 for details.

Cluster Configuration

Cluster configurations are settings that are replicated cluster-wide and every HA member is configured with the same cluster configuration information. The Central Management and Cluster Management components use cluster information to provide rapid failover without loss to critical policy and configuration information.

The cluster configuration file, `cluster.ini`, is stored in the `/etc/iscan` folder and is used to store the HA cluster settings. You can configure the following elements of a cluster through the Web console Cluster Management page:

- **Cluster Name—**The name of the cluster
- **Cluster Description—**The description of the cluster
- **Cluster IP Address—**The floating management IP address of the cluster is always associated with the active node
- **Weighted Priority Election—**Enable or disable (default)
- **Cluster Members—**The list of the nodes belonging to the HA cluster with login access provided to child node.

Note: For this version of IWSVA, the following items are not configurable:
- Cluster Deployment Mode—Always Transparent Bridge mode.
- HA Mode—Always active/passive.

Node Configuration

Node configuration settings are applied to a specific HA member and are not cluster-wide settings. These node-specific settings are never synchronized between the HA members. Node specific settings include the following:

- **Hostname—**The name of the node
- **Role**—Either parent or child

- **IP Address—**The IP address used on the heartbeat port. If this is empty, a new IP will be negotiated between the cluster members and written to the IP address parameter.
- **Weight—**The weight of the node. Valid values are 1-255. The higher the weight, the greater the chance the node will be selected to act as the parent node.
- **Status**—Status of the node. Green is up, red is down.
- **Last Synchronization**—Gives the date and time of the last successful synchronization
- **Synchronization Status**—Green is successful, red is failed. If failed, a reason displays in the tooltip.

Cluster Logs and Notifications

The HA cluster logs and records the following events:

- Creating a cluster
- Dissolving or breaking apart an existing cluster
- Adding a member to a cluster
- Changing the configuration of a cluster
- Removing a member from a cluster
- Changing the role of a cluster member
- Performing manual synchronization
- Failing over
- Detecting an abnormality

Cluster notifications are issued when:

- Abnormalities are detected
- A failover occurs
- A member is restored
- A failover or switchover cannot be performed

Accessing the Cluster

To access the parent node:

Administrators can access the parent member's Web management interface through one of two IP addresses:

- the parent member's management IP address and port number
- the Cluster IP address and port number

Example:

```
http://<parent management IP address>:<portnumber>
```

```
http://<cluster IP address>:<portnumber>
```

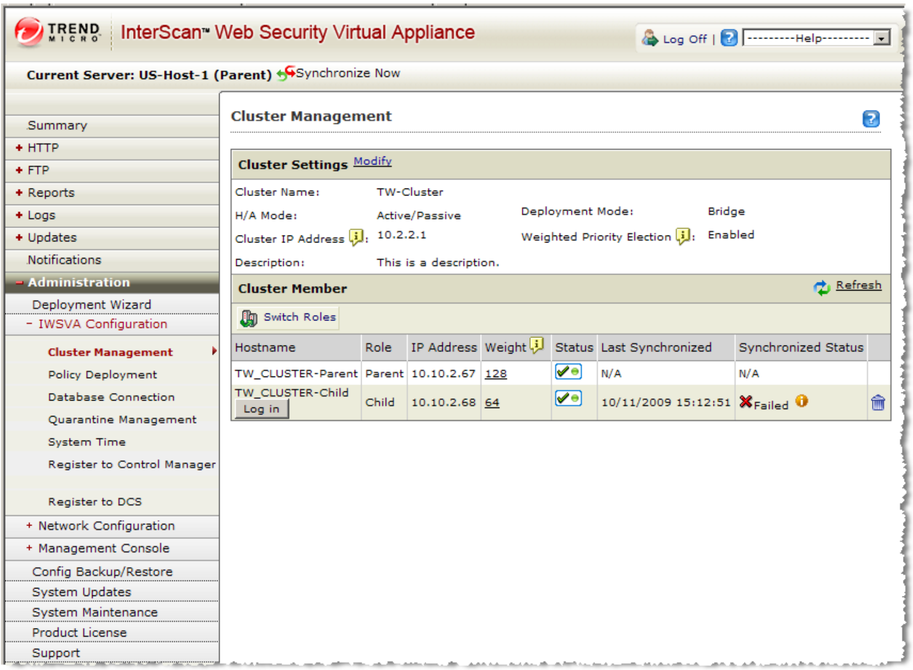
To access the child node:

Administrators can log into the Web management console of the child node two ways:

- Through the link on the Cluster Management page (**Administration > IWSVA Configuration > Cluster Management > Login** button for child node)
- Through the management port IP address of the child node

Example:

```
http://<child node IP address>:<portnumber>
```



Cluster Management

Cluster Settings

Cluster Name: TW-Cluster
H/A Mode: Active/Passive
Deployment Mode: Bridge
Cluster IP Address: 10.2.2.1
Weighted Priority Election: Enabled
Description: This is a description.

Cluster Member

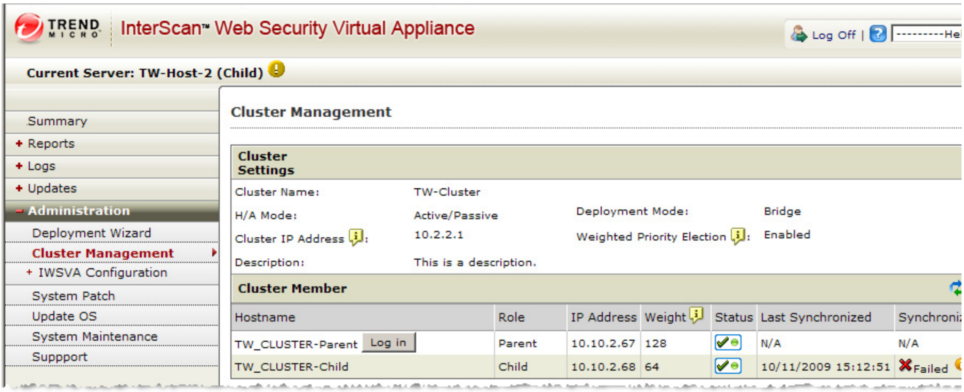
Hostname	Role	IP Address	Weight	Status	Last Synchronized	Synchronized Status
TW_CLUSTER-Parent	Parent	10.10.2.67	128	✓	N/A	N/A
TW_CLUSTER-Child	Child	10.10.2.68	64	✓	10/11/2009 15:12:51	✗Failed

FIGURE 3-2. Parent Node Cluster Management Page has Child Node Login Access

To protect against accidental configuration, all cluster-level features are hidden or blocked in the child member's Web management interface. (Compare the parent node left menu in *Figure 3-2* with the child node left menu in *Figure 3-3*.) Only the child member applicable configuration parameters that apply specifically to the child member are exposed and configurable through the child member's Web management interface. *Table 3-1* gives a detailed list of child-level settings and features.

If administrators need to change cluster-level settings while logged into the child member, they can simply login to the parent member through the “Login” button posted beside the parent member on the Cluster Management screen.

IWSVA HA uses single sign-on technology to pass authentication credentials between cluster members so typing a password to access other members are not necessary.



Current Server: TW-Host-2 (Child)

Cluster Management

Cluster Settings

Cluster Name: TW-Cluster

H/A Mode: Active/Passive

Deployment Mode: Bridge

Cluster IP Address: 10.2.2.1

Weighted Priority Election: Enabled

Description: This is a description.

Cluster Member

Hostname	Role	IP Address	Weight	Status	Last Synchronized	Synchroni
TW_CLUSTER-Parent	Parent	10.10.2.67	128	✓	N/A	N/A
TW_CLUSTER-Child	Child	10.10.2.68	64	✓	10/11/2009 15:12:51	✗Failed

FIGURE 3-3. Child node Cluster Management page with access to the parent node.

Note: CLI commands for centrally managed features are not available on the child node.

Cluster Management Web Console Page

From the Cluster Management page at **Administration > IWSVA Configuration > Cluster Management**, administrators can configure the following:

- Deleting a Child Member from a Cluster on page 3-16
- Dissolving a Cluster on page 3-16
- Performing a Manual Switchover on page 3-17
- Synchronizing Nodes Manually on page 3-7
- Modifying a Cluster on page 3-17

Deleting a Child Member from a Cluster

If you delete a child node from a cluster, the cluster still exists with the parent node as the only member. Another node can be added later as a child node.

To delete a child node:

1. Go to **Administration > IWSVA Configuration > Cluster Management** in the parent member Web console.
2. Go the **Cluster Member** section of the page.
3. Click the delete icon (🗑) in the child row to delete the child member.
4. Click **OK** to confirm the deletion. A progress bar displays.
5. If, after a few second, if the deletion has not completed, click your browser's **Refresh** button.

   The child member no longer displays in the Cluster Member list and the former child node will return to Forward Proxy mode.

Dissolving a Cluster

Dissolving an HA cluster breaks apart the HA cluster and occurs after the child member and parent member have been deleted. Dissolving an HA cluster returns the active HA member to a standalone IWSVA device operating in Transparent Bridge mode.

To dissolve a cluster:

1. Go to **Administration > IWSVA Configuration > Cluster Management** in the parent member Web console.
2. Delete the child member of the cluster as shown in Deleting a Child Member from a Cluster on page 3-16.
3. In the **Cluster Member** section of the page, click the delete icon (🗑) to delete the parent member.
4. Click **OK** to confirm the dissolution. A progress bar displays.

   a. If, after five minutes, if the dissolution has not completed, click your browser's **Refresh** button.

      The parent member become a standalone IWSVA unit in Transparent Bridge mode and the Cluster Management page no longer displays.

Performing a Manual Switchover

Administrators can manually switch the parent/child roles of the two members in an HA cluster. After a successful switchover, the original parent member becomes the child member and goes into passive mode. The original child member becomes the parent member and goes into active mode.

Note: Administrators can only perform a manual switchover if the Weighted Priority Election process is disabled. To perform a switchover with Weighted Priority Election mode enabled, administrators must modify the weight of each member to trigger an HA switchover. See Modifying a Cluster on page 3-17 for details on changing the weight value for a cluster member.

To perform a manual switchover with Weighted Priority Election mode disabled:

Note: If IWSVA is performing a synchronization, either a manually or a scheduled synchronization, the Synchronized Status shows “Syncing …”, and manual switchovers are prevented. This applies to switchovers when the Weight Priority Election mode is disabled (by switching roles) or if attempting to change the weight value of a node with the Weighted Priority Election mode enabled. Automatic failovers still occur even if synchronization is in progress, reverting to the policies and deployment settings that existed after the most recent successful synchronization.

1. Go to **Administration > IWSVA Configuration > Cluster Management** in the parent node Web console.
2. In the Cluster member section, click **Switch Roles**.
3. Click **OK** in the confirmation to switch roles and be re-logged into the new parent node.

Modifying a Cluster

The Cluster Management page allows administrators to view cluster settings, modify cluster settings, and to switch roles between parent and child servers.

Table 3-2 shows the Cluster Settings displayed on the Cluster Management page.

TABLE 3-2. Cluster Settings

VALUE	DESCRIPTION
Cluster Name	This is the name assigned to the cluster when it was first created in the Deployment Wizard. (Modifiable)
HA Mode	Active/Passive (Not modifiable)
Cluster IP Address	The floating IP address used to log into the cluster from the Web console or CLI. This IP address remains the same, even after a switchover occurs. (Modifiable)
Description	Displays the (optional) description entered when the cluster was added through the Deployment Wizard. (Modifiable)
Deployment Mode	Currently, this parameter always displays "Bridge" because IWSVA HA clusters are only supported in Transparent Bridge mode. (Not modifiable)
Weighted Priority Election	Displays either Enabled or Disabled. (Modifiable)
Switch Roles	Allows administrators to switch roles between parent and child members.
Refresh	Updates the status of cluster members

This Cluster Members section of the Cluster Management page displays the cluster members (parent and child members), gives status details, and allows login access to the child node.

Table 3-3 shows the parameters displayed for both parent and child nodes.

TABLE 3-3. Cluster Member Settings

PARAMETER	DESCRIPTION
Hostname	Displays the server name
Role	Displays either Parent or Child
IP Address	Displays the IP address of the device.
Weight	Displays the weight entered when the cluster was configured. (Default: parent 128/child 64- Modifiable)
Status	Displays the following icons: ✓ ● Up status ✗ ● Down status
Last Synchronized	Displays the date and time (hours: minutes: seconds) when the child server was last synchronized with the parent.
Synchronization Status	Displays the following: N/A ✓ Successful — Success ✗ Failed ⓘ — Failed. If failed, an information tool tip displays the reason why the synchronization failed.
Dissolve	Displays an icon (🗑) to delete the child member. The icon only displays for the parent member if the child member has been deleted. Deleting the parent member dissolves the whole cluster.

To modify cluster settings:

1. Go to **Administration > IWSVA Configuration > Cluster Management.**
2. Click the **Modify** link by the Cluster Settings heading.
3. In the Cluster Settings page, modify the following parameters as needed:
    - **Cluster Name**—Displays the name assigned to the cluster when it was first created in the Deployment Wizard. (Modifiable)
    - **Description**—Displays the (optional) description, if any, entered when the cluster was added through the Deployment Wizard. (Modifiable)
    - **Floating IP Address**—Displays the floating management (or cluster) IP address used to log into the cluster from the Web console or CLI. The floating IP address is always associated with the active node in the cluster. (Modifiable)
    - **Weighted Priority Election**—Displays either Enabled or Disabled. If the Weighted Priority Election value is set to enable, the HA pair launches an election to choose the maximum weighted machine. If the Weighted Priority Election value is set to disable, the HA pair only launches an election when the current active (or primary) machine is not available. (Modifiable)
    - **HA Mode**—Active/Passive (Display only)
    - **Deployment Mode**—Currently, this parameter always displays **"**Bridge**"** because IWSVA HA clusters are only supported in Transparent Bridge mode. (Display only)
4. Click **Save**.

To change the weight value of a node:

Note: The Weighted Priority Election mode must be set to Enable to perform the following procedure. (To enable the Weight Priority Election mode, see To modify cluster settings: on page 3-20, Step 3.) Roles can be switched manually if the Weighted Priority Election is disabled. See Performing a Manual Switchover on page 3-17 for details.

1. Go to **Administration > IWSVA Configuration > Cluster Management.**
2. In the Cluster Members section, click the weight value to be changed.
3. In the Weight screen, change the weight value to reflect the appropriate value. (1-255, higher value = higher priority.)

4. Click **Save**.

   If you change a child member's weight value to be greater than the parent member's weight value, and the Weighted Priority Election has been enabled, roles for the two members will be switched.

Chapter 4

Updates

Because new malicious programs and offensive Web sites are developed and launched daily, it is imperative to keep your software updated with the latest pattern files and engines, as listed on the Updates Schedule page on the InterScan™Web Security Virtual Appliance (IWSVA) Web console.

Topics in this chapter include the following:

Product Maintenance

From time to time, Trend Micro might release a patch for a reported known issue or an upgrade that applies to your product. To find out whether there are any patches available, visit the following URL:

`http://downloadcenter.trendmicro.com`

Clicking the link for IWSVA takes you to the Update Center page for IWSVA.

Enter the following search criteria:

- **Category:** Internet Gateway
- **Product:** InterScan Web Security Virtual Appliance
- **Version:** Current product version

Patches are dated. If you find a patch that you have not applied, open the readme document to determine whether the patch applies to you. If so, follow the upgrade instructions in the readme.

Renewing Your Maintenance Agreement

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which you must purchase renewal maintenance.

If your Maintenance Agreement expires, scanning is still possible, but virus pattern and program updates stop. To prevent this, renew the Maintenance Agreement as soon as possible.

To purchase renewal maintenance, contact the same vendor from whom you purchased the product. A Maintenance Agreement, extending your protection for a year, is sent by post to the primary company contact listed in your company's Registration Profile.

To view or modify your company's Registration Profile, log into the account at the Trend Micro online registration Web site:

`https://olr.trendmicro.com/registration`

To view your Registration Profile, type the Logon ID and Password created when you first registered your product with Trend Micro (as a new customer), and click **Login**.

About ActiveUpdate

ActiveUpdate is a service common to many Trend Micro products. ActiveUpdate connects to the Trend Micro Internet update server to enable downloads of the latest pattern files and engines.

ActiveUpdate does not interrupt network services, or require you to reboot your computers. Updates are available on a regularly scheduled interval that you configure, or on demand.

Updating From the IWSVA Web Console

If you are not using Trend Micro Control Manager for centralized administration of your Trend Micro products, IWSVA polls the ActiveUpdate server directly. Updated components are deployed to IWSVA on a schedule you define, such as the following:

- Minutes (15, 30, 45, 60)

  These 15-minute interval updates only apply to virus, spyware, phish, URL Filtering page analysis, IntelliTrap, and IntelliTunnel patterns.
- Hourly
- Daily
- Weekly
- On demand (manually)

Note: Trend Micro recommends hourly updates of the pattern files and daily and weekly updates of engines. All updates include the following patterns: virus, spyware, phish, URL Filtering page analysis, IntelliTrap, and IntelliTunnel patterns.

Proxy Settings for Updates

If you use a proxy server to access the Internet, you must enter the proxy server information into the IWSVA Web console before attempting to update components. Any proxy information that you enter is used for the following:

- Updating components from Trend Micro's update servers
- Product registration and licensing

- Web reputation queries

To configure a proxy server for component and license updates:

1. Open the IWSVA Web console and click **Updates > Connection Settings**.
2. Select "**Use a proxy server for pattern, engine, license updates and Web Reputation queries**" to specify a proxy server or port.
3. If your proxy server requires authentication, type a user ID and password in the fields provided.

   Leave these fields blank if your proxy server does not require you to authenticate.
4. In the **Pattern File Setting** section, type the number of pattern files to keep on the IWSVA device after updating to a new pattern (default and recommended setting is three pattern files).

   Keeping old pattern files on your server allows you to roll back to a previous pattern file in the event of an incompatibility with your environment; such as excessive false positives. When the number of pattern files on the server exceeds your configuration, the oldest pattern file is automatically deleted.
5. Click **Save**.

Note: In transparent bridge mode, the IWSVA has an internal interface and an external interface. To ensure updates function properly, the configuration of the ActiveUpdate proxy and server settings must be done on the same side. If IWSVA is deployed with other proxy servers, the next hop proxy settings for the ActiveUpdate proxy and server should be the same server on the same side of the interface.

Updatable Program Components

To ensure up-to-date protection against the latest risks, there are several components you can update:

- **Pattern files**—These files are: Virus, phish spyware/grayware, URL filtering page analysis, IntelliTrap, and IntelliTrap Exceptions. These files contain the binary "signatures" or patterns of known security risks. When used in conjunction with the scan engine, IWSVA is able to detect known risks as they pass through the Internet gateway. New virus pattern files are typically released at the rate of several per week, while the Phish and grayware/spyware pattern files are updated less frequently.

- **IntelliTunnel signature definition file**—This file contains "signatures" of certain HTTP interactions (such as instant messaging protocols tunneled through HTTP and SSL authentication requests) that you might wish to control. New signature definition files are typically released a few times a year as the covered protocols evolve or new types of HTTP interactions are added. See IntelliTunnel Security on page 7-44.

Note: The IntelliTunnel feature is unrelated to the virus scanning facility and uses its own scanning engine, which is not dynamically updatable.

- **Virus scan engine**—This module analyzes each file's binary patterns and compares them against the binary information in the pattern files. If there is a match, the file is determined to be malicious.
- **URL Filtering Engine**—IWSVA utilizes the Trend Micro URL Filtering Engine to perform URL categorization and reputation rating based on the data supplied by the Trend Micro Web Reputation feature. Trend Micro recommends using the default setting of a weekly update check to ensure that your installation has the most current URL Filtering Engine.

Virus Pattern File

The Trend Micro scan engine uses an external data file, called the virus pattern file, to keep current with the latest viruses and other Internet risks such as Trojans, mass mailers, worms, and mixed attacks. New virus pattern files are created and released several times a week, and any time a particularly pernicious risk is discovered.

All Trend Micro antivirus programs using the ActiveUpdate feature (see About ActiveUpdate starting on page 4-3 for details) can detect whenever a new virus pattern is available at the server, and can be scheduled to automatically poll the server every hour, day, week, and so on, to get the latest file. Virus pattern files can also be manually downloaded from the following Web site:

```
http://www.trendmicro.com/download/pattern.asp
```

There, you can find the current version, release date, and a list of the new virus definitions included in the file.

How it Works

The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Because each virus contains a unique binary "signature" or string of tell-tale characters that distinguishes it from any other code, the virus experts at TrendLabs capture inert snippets of this code to include in the pattern file. The engine then compares certain parts of each scanned file to the data in the virus pattern file looking for a match.

Pattern files use the following naming format:

```
lpt$vpn.###
```

where ### represents the pattern version (for example, 400). To distinguish a given pattern file with the same pattern version and a different build number, and to accommodate pattern versions greater than 999, the IWSVA Web console displays the following format:

```
roll number.pattern version.build number (format: xxxxx.###.xx)
```

- `roll number`—This represents the number of rounds when the pattern version exceeds 999 and could be up to five digits.
- `pattern version`—This is the same as the pattern extension of `lpt$vpn.###` and contains three digits.
- `build number`—This represents the patch or special release number and contains two digits.

If multiple pattern files exist in the same directory, only the one with the highest number is used. Trend Micro publishes new virus pattern files on a regular basis (typically several times per week), and recommends configuring a hourly automatic update on the **Updates > Schedule** screen. Updates are available to all Trend Micro customers with valid maintenance contracts.

Note: There is no need to delete the old pattern file or take any special steps to "install" the new one.

Phish Pattern File

As new "phishing" scams that attempt to steal personal data through counterfeit versions of legitimate Web sites are discovered, Trend Micro collects their URLs and incorporates the information into the Phish pattern file. The Phish pattern file is saved in `/etc/iscan/phishB.ini` and contains an encrypted list of known phishing URLs.

Page Analysis Pattern

URL filtering page analysis pattern is used by the URL filtering engine to perform local page analysis and adjust the final reputation score of a visited Web page. If the result of the analysis indicates that the Web page contains malicious content, IWSVA automatically decreases its reputation score and returns the revised score to the reputation server.

The URL filtering page analysis pattern file is stored in the following directory:

```
/etc/iscan/Ctx#####.###
```

Spyware/Grayware Pattern File

As new hidden programs (grayware) that secretly collect confidential information are written, released into the public, and discovered, Trend Micro collects their tell-tale signatures and incorporates the information into the spyware/grayware pattern file. The spyware/grayware pattern file is stored in the following directory:

```
/etc/iscan/ssaptn.###
```

where ### represents the pattern version. This format distinguishes a given pattern file with the same pattern version and a different build number. It also accommodates pattern versions greater than 999. The IWSVA Web console displays the following format:

```
roll number.pattern version.build number (format: xxxxx.###.xx)
```

- `roll number`—This represents the number of rounds when the pattern version exceeded 999 and could be up to five digits.
- `pattern version`—This is the same as the pattern extension of `ssaptn.###` and contains three digits.
- `build number`—This represents the patch or special release number and contains two digits.

IntelliTrap Pattern and IntelliTrap Exception Pattern Files

IntelliTrap detection uses a scan option in the Trend Micro's virus scanning engine with IntelliTrap pattern (for potentially malicious files) and IntelliTrap Exception pattern (as an allowed list). IWSVA uses the IntelliTrap option and patterns available for detecting malicious compressed files, such as bots in compressed files. Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides a heuristic evaluation of compressed files to help reduce the risk that a bot or any other malicious compressed file might cause to a network.

IntelliTrap pattern `tmblack.###` and IntelliTrap exception pattern `tmwhite.###` are saved in the `/etc/iscan/` directory.

Scan Engine

At the heart of all Trend Micro antivirus products lies a proprietary scan engine. Originally developed in response to the first computer viruses the world had seen, the scan engine today is exceptionally sophisticated. It is capable of detecting Internet worms, mass-mailers, Trojan horse risks, network exploits and other risks, as well as viruses. The scan engine detects the following types of risks:

- "in the wild," or actively circulating
- "in the zoo," or controlled viruses that are not in circulation, but are developed and used for research and "proof of concept"

In addition to having perhaps the longest history in the industry, the Trend Micro scan engine has also proven in tests to be one of the fastest—whether checking a single file, scanning 100,000 files on a desktop machine, or scanning email traffic at the Internet gateway. Rather than scan every byte of every file, the engine and pattern files work together to identify not only tell-tale characteristics of the virus code, but the precise location within a file where the virus would hide. If a virus is detected, it can be removed and the integrity of the file restored.

To help manage disk space, the scan engine includes an automatic clean-up routine for old viruses, spyware, and IntelliTrap pattern files as well as incremental pattern file updates to help minimize bandwidth usage.

In addition, the scan engine is able to decode all major internet encoding formats (including MIME and BinHex). It also recognizes and scans common compression formats, including Zip, Arj, and Cab. Most Trend Micro products also allow administrators to determine how many layers of compression to scan (up to a maximum of 20), for compressed files contained within a compressed file.

It is important that the scan engine remains current with the latest risks. Trend Micro ensures this in two ways:

- Frequent updates to the scan engine's data file, called the virus pattern file, which can be downloaded and read by the engine without the need for any changes to the engine code itself.
- Technological upgrades in the engine software prompted by a change in the nature of virus risks, such as the rise in mixed risks like Italian Job.

In both cases, updates can be automatically scheduled, or an update can be initiated on demand.

The Trend Micro scan engine is certified annually by international computer security organizations, including the International Computer Security Association (ICSA).

About Scan Engine Updates

By storing the most time-sensitive virus information in the virus pattern file, Trend Micro is able to minimize the number of scan engine updates, while at the same time keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. New engines are released, for example, when:

- New scanning and detection technologies have been incorporated into the software
- A new, potentially harmful virus is discovered that cannot be handled by the current engine
- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats

To view the version number for the most current version of the scan engine, visit:

`http://www.trendmicro.com`

Web Reputation Database

The Web Reputation database resides on a remote server. When a user attempts to access a URL, IWSVA retrieves information about this URL from the Web Reputation database and stores it in the local cache. Having the Web Reputation database on a remote server and building the local cache with this database information reduces the overhead on IWSVA and improves performance.

The following are the information types the Web Reputation database can retrieve for a requested URL:

- Web category
- Pharming and phishing flags used by anti-pharming and anti-phishing detection
- Web Reputation scores used to block URL access, based on a specified sensitivity level (see Specifying Web Reputation Rules on page 7-13)

The Web Reputation database is updated with the latest categorization of Web pages.

If you believe the reputation of a URL is misclassified or you want to know the reputation of a URL, please use the link below to notify Trend Micro:

```
http://reclassify.wrs.trendmicro.com/submit-files/wrsonlinequery.asp
```

Incremental Updates of the Pattern Files and Engines

ActiveUpdate supports incremental updates of the latest pattern and engine files. Rather than downloading the entire 35 MB file each time, ActiveUpdate can download only the portion of the file that is new and append it to the existing file. This efficient update method can substantially reduce the bandwidth needed to update your antivirus software, deploy pattern, and engine files throughout your environment.

Component Version Information

To know which pattern file, scan engine, or application build you are running, click **Summary** in the main menu. The version in use is shown in the **Current Version** column on the **System Dashboard** tab.

Manual Updates

The effectiveness of IWSVA depends upon using the latest pattern and engine files. Signature-based virus and spyware/grayware scanning works by comparing the binary patterns of scanned files against binary patterns of known risks in the pattern files. Trend Micro frequently releases new versions of the virus pattern and spyware pattern in response to newly identified risks. Similarly, new versions of the Phish pattern are released as new phishing URLs are identified.

New versions of the Trend Micro scan engine are updated as performance is improved and features added to address new risks.

Note: If Internet connections on your network pass through a proxy server, you need to configure your proxy information. Click **Updates > Connection Settings** from the main menu and enter your proxy server information.

To update the engines and pattern files:

1. Click **Summary** on the main menu and make sure the **System Dashboard** tab is active.
2. Click **Update**.
3. For all of the components listed in the Manual Update screen, click one of the following:
   - **Update All**—Updates all components
   - **Update**—Updates only the selected component

   If IWSVA is already using the latest version of the component and no update is available, no component is updated. Forcing an update (by clicking **Update**) is not necessary unless the components on the IWSVA device are corrupt or unusable.

Forced Manual Updates

IWSVA provides an option to force an update to the pattern file and the scan engine when the version on IWSVA is greater than or equal to its counterpart on the remote download server (normally IWSVA would report that no updates are available). This feature is useful when a pattern file or scan engine is corrupt and you need to download the component again from the update server.

To force an update of a pattern file or scan engine:

1. Click **Updates > Manual** on the main menu. Alternatively, clicking **Update** in the System Dashboard screen to display the Manual Update screen.
2. For all of the components listed, click **Update** to update only the selected component(s)

   A message box appears if the version of the pattern file or scan engine on IWSVA is greater than or equal to the counterpart on the remote download server. If the pattern file on IWSVA is older than the one on the remote download server, the newer pattern file is downloaded.
3. Click **OK** in the message box to start the forced update.

Scheduled Updates

IWSVA can perform scheduled updates for the following pattern files:

- Virus
- Spyware
- URL page analysis
- Phish Pattern
- IntelliTrap
- IntelliTunnel

Likewise, IWSVA can perform scheduled updates for the Scan and URL Filtering engines.

To schedule automatic pattern file and engine updates:

1. Click **Updates > Schedule** on the main menu.
2. For each type of updatable component, select the update interval.

   The following are your options:

   - Every *x* minutes (pattern files only; select the number of minutes between update interval)
   - Hourly (pattern files only)
   - Daily

- Weekly (select a day from the drop-down menu; this is the recommended setting for the latest engine updates)

Note: Scheduled updates for a given component can be disabled by selecting **Manual updates only** in each component section.

3. For each component, select a **Start time** for the update schedule to take effect.
4. Click **Save**.

Note: Use the **Summary** screen in the IWSVA Web console to verify the current version of a pattern file. If your network configuration includes a cache server, Trend Micro recommends that you clear the cache and reboot the cache server after updating the pattern file. This forces all URL requests to be scanned, ensuring better network protection. Consult your cache server documentation for information on how to clear the cache and reboot the server.

Maintaining Updates

Verifying a Successful Update

The **System Dashboard** tab of the **Summary** screen in the IWSVA Web console displays the version of the component in use, plus the time and date of the last update. Check the Summary page to verify that a manual or scheduled update has completed successfully.

Update Notifications

IWSVA can issue notifications to proactively inform an administrator about the status of a pattern or engine update. For more information about configuring update-related notifications, see Enabling Pattern File Update Notifications starting on page 12-50 and Enabling Notifications for URL Filtering Engine and Scan Engine Updates starting on page 12-53.

Rolling Back an Update

IWSVA checks the program directory and uses the latest pattern file and engine library file to scan inbound/outbound traffic. It can distinguish the latest pattern file by its file extension; for example, `lpt$vpn.401` is newer than `lpt$vpn.400`.

Occasionally, a new pattern file might incorrectly detect a non-infected file as a virus infection (known as a "false positive"). You can revert to the previous pattern file or engine library file.

Note: IWSVA does not support rollback for the URL filtering engine.

To roll back to a previous pattern file or scan engine:

1. Click **Updates > Manual** on the main menu.
2. Select the component to roll back and click **Rollback**.

   A progress bar indicates the rollback progress, and a message screen then displays the outcome of the rollback. After the rollback, you can find the current version and date of the last update on the **System Dashboard** tab of the **Summary** screen.

Deleting Old Pattern Files

After updating the pattern file, IWSVA keeps old pattern files (Virus, Spyware, IntelliTrap, and IntelliTrap Exception pattern files) on the server so they are available to accommodate a roll back. The number of pattern files kept on the server is controlled by the "**Number of pattern files to keep"** setting on the **Updates > Connection Settings** page.

If you need to manually delete pattern files, they can be found in the `/etc/iscan/` directory of IWSVA.

Controlled Virus Pattern Releases

There are two release versions of the Trend Micro virus pattern file:

- The Official Pattern Release (OPR) is Trend Micro's latest compilation of patterns for known viruses. It is guaranteed to have passed a series of critical tests to ensure that customers get optimum protection from the latest virus risks. Only OPRs are available when Trend Micro products poll the ActiveUpdate server.
- A Controlled Pattern Release (CPR) is a pre-release version of the Trend Micro virus pattern file. It is a fully tested, manually downloadable pattern file, designed to provide customers with advanced protection against the latest computer viruses and to serve as an emergency patch during a virus risk or outbreak.

Note: After you apply a CPR, incremental updates are not possible. This means that subsequent updates require downloading the entire pattern file rather than just the new patterns, resulting in a slightly longer pattern download time.

In order for IWSVA to access the new pattern file, ensure that it has the same permission and ownership as the previous pattern file.

To apply the latest CPR to IWSVA:

1. Open `http://www.trendmicro.com/download/pattern-cpr-disclaimer.asp` and click **Agree** to signify your agreement with the terms and conditions of using a Trend Micro CPR.
2. Download the CPR to a temporary folder on the IWSVA device. The filename is in the form `lptXXX.zip`.
3. Stop all IWSVA services.
4. Extract the contents of the files that you downloaded to the `/etc/iscan/`directory of IWSVA.
5. Restart all IWSVA services.

   To verify that the CPR was applied correctly, click **Summary** in the main menu; then, click the **System Dashboard** tab and confirm that the virus pattern version in use corresponds to the version of the CPR that you tried to apply.

Chapter 5

HTTP Configuration

Before you start using InterScan Web Security Virtual Appliance (IWSVA) to scan for malicious HTTP(S) downloads, filter or block URLs, and apply access quotas for your clients, you need to configure some HTTP settings that control the HTTP traffic flow. IWSVA can be used in conjunction with another proxy server on your network; alternatively, you can configure IWSVA to use its native proxy.

Note: - To enable and configure WCCP, see Network Configuration and Load Handling on page 5-11 and your Cisco product documentation.
- To enable and configure Full Transparency (Transparent Bridge mode), see Network Configuration and Load Handling on page 5-11.

Topics in this chapter include the following:

Enabling the HTTP(s) Traffic Flow

The deployment mode is originally configured with the IWSVA Deployment Wizard. If you would like to change the deployment mode after the installation, you can use the **Administration > Deployment Wizard** to make the changes.

To enable or disable the HTTP(s) traffic flow through IWSVA:

1. Select **Summary** on the main menu.

   The state of HTTP(s) traffic flowing through IWSVA appears at the top of the Scanning page.
2. Select one of the following:
   - If HTTP(s) traffic is turned off, click the **Turn On** link to enable it.
   - If HTTP(s) traffic is turned on, click the **Turn Off** link to disable it.

When HTTP(s) traffic is turned off, your clients cannot access Web sites or any other services carried through HTTP(s).

Specifying a Proxy Configuration and Related Settings

If you would like to change the deployment mode after the installation, you can use the **Administration > Deployment Wizard** to make changes.

- **Transparent bridge**—IWSVA acts as a Layer 2 network bridge between the devices it is deployed between and transparently scans HTTP(S) and FTP traffic between the clients and external services. No configuration changes to the network devices are required. Transparent bridge settings apply to both HTTP and FTP traffic, and if selected, FTP proxy settings are disabled. By default, SSL (HTTPS) traffic is passed through IWSVA, but not scanned. To allow IWSVA to scan SSL-encrypted traffic, you can configure HTTPS decryption policies to decrypt the content before scanning.

  If the clients and IWSVA are in the same segment, no configuration is required. Otherwise, see the following list for mixed segment configuration considerations.

  If the network device and IWSVA device are on different network segments, use the IWSVA routing table to point IWSVA to the device.

- **Forward Proxy**—This configuration is used to protect clients from receiving malicious HTTP-borne risks from a server. This is the most common configuration, and the typical use case is to protect Web users on your network from receiving malicious Internet downloads. IWSVA and the clients that it protects are typically in the same LAN.
- **Reverse proxy**—This configuration is used to protect Web and FTP servers from attacks or malware introduced by public or private users.
- **ICAP**—Choose this topology if you have an ICAP client on the network and you want it to pass traffic to IWSVA for scanning. IWSVA acts as an ICAP server.
- **WCCP**—The WCCP configuration allows customers that have WCCP enabled routers and switches to redirect Web and FTP traffic to IWSVA to create a high-performance scalable and redundant architecture.

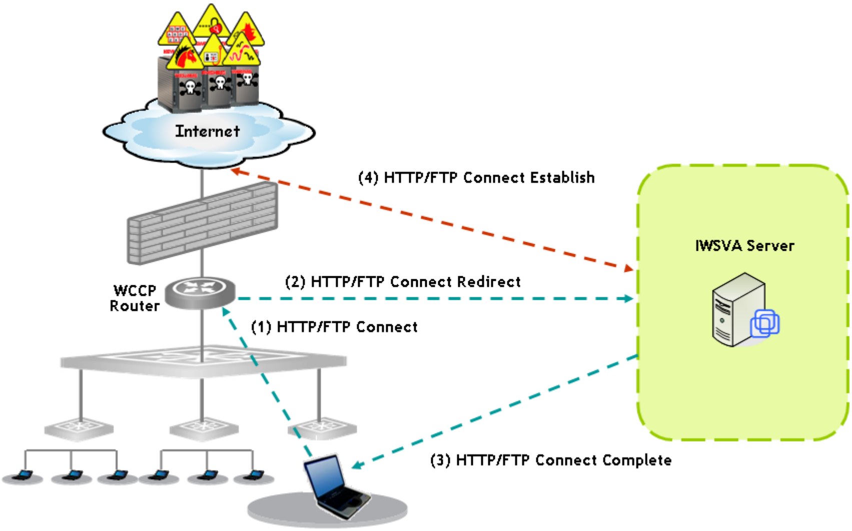

Internet
(4) HTTP/FTP Connect Establish
IWSVA Server
WCCP Router
(2) HTTP/FTP Connect Redirect
(1) HTTP/FTP Connect
(3) HTTP/FTP Connect Complete

FIGURE 5-1. WCCP configuration and Web and FTP traffic

Proxy Configurations

There are several types of proxy configurations:

- No upstream proxy (stand-alone mode)
- Upstream proxy (dependent mode)
- Simple transparency
- Reverse proxy
- WCCP

No Upstream Proxy (Stand-alone Mode)

The simplest configuration is to install IWSVA in stand-alone mode, with no upstream proxy. In this case, IWSVA acts as a proxy server for the clients. The advantages of this configuration are its relative simplicity and that there is no need for a separate proxy server. A drawback of a forward proxy in stand-alone mode is that each client must configure the IWSVA device as their proxy server in their browser’s Internet connection settings. This requires cooperation from your network users, and also makes it possible for users to exempt themselves from your organization’s security policies by reconfiguring their Internet connection settings.

Note: If you configure IWSVA to work in stand-alone mode, each client on your network needs to configure Internet connection settings to use the IWSVA device and port (default 8080) as their proxy server.

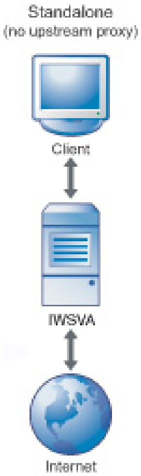


FIGURE 5-2. Forward, no upstream proxy

To configure a stand-alone installation:

1. Click **Administration > Deployment Wizard** from the main menu.

   The Deployment Wizard displays.
2. Ensure that **Forward proxy mode** is selected, can click **Next**.
3. Verify that **Enable upstream proxy** and **Enable transparency** are not selected.
4. Click **Next** until the Submit button displays. Click **Submit.** Click **Close**.

Upstream Proxy (Dependent Mode)

IWSVA can be configured to work in conjunction with another proxy server on your network. In this configuration, IWSVA passes requests from clients to another proxy server, which forwards the requests to the requested server.

Like the stand-alone mode, the dependent mode proxy configuration also requires client users to configure the IWSVA device as their proxy server in their Internet connection settings. One benefit of using an upstream proxy is improved performance through content caching on the upstream proxy server. IWSVA does not perform any content caching, so every client request needs to contact the Internet server to retrieve the content. When using an upstream proxy, pages cached on the proxy server are served more quickly.

Note: If IWSVA is configured to operate in upstream proxy mode with a designated proxy server, Trend Micro recommends that the proxy settings for Updates also be configured to the same designated proxy server (see Proxy Settings for Updates on page 4-3). Certain types of update events utilize the Updates proxy settings to retrieve important information. If proxy settings are not configured properly, IWSVA will not be able to access the Internet for these services.

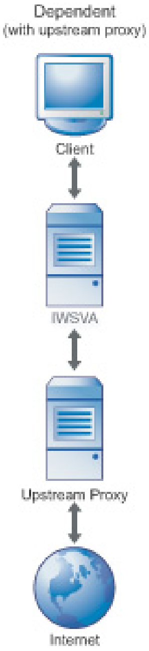


FIGURE 5-3. Forward, upstream proxy

Note: When IWSVA is configured in HTTP Forward Proxy mode with Upstream Proxy enabled, pharming sites cannot be effectively blocked.

When you configure IWSVA to work in Forward Proxy mode and enable Upstream Proxy, the Server IP White List will not take effect. Content from servers that you configure on the Server IP White List still will be scanned or filtered.

To configure IWSVA to work with an upstream proxy:

1. Click **Administration > Deployment Wizard** from the main menu.

   The Deployment Wizard displays.
2. Ensure that **Forward proxy mode** is selected, can click **Next**.
3. Check **Enable upstream proxy** and enter the IP address or host name of the upstream **Proxy server**, and the **Port number**.
4. Click **Next** until the Submit button displays. Click **Submit.** Click **Close**.

Transparent Proxy

Transparency is the functionality whereby client users do not need to change their Internet connection's proxy settings to work in conjunction with IWSVA. Transparency is accomplished with a Layer 4 switch that redirects HTTP packets to a proxy server, which then forwards the packets to the requested server.

IWSVA supports a "simple" type transparency. Simple transparency is supported by most Layer 4 switches. While it is compatible with a wide variety of network hardware from different manufacturers, configuring simple transparency does impose several limitations:

- When using simple transparency, the User Identification method to define policies is limited to IP address and/or host name; configuring policies based on LDAP is not possible.
- FTP over HTTP is not available; thus, links to ftp:// URLs might not work if your firewall settings do not allow FTP connections. Alternatively, links to ftp:// URLs might work, but the files are not scanned.
- Simple transparency is not compatible with some older Web browsers when their HTTP requests do not include information about the host.

- Do not use any source NAT (IP masquerade) downstream of IWSVA, because IWSVA uses the IP address of the client to scan and clean the malicious traffic.
- A DNS server is needed for DCS to resolve the client machine name from its IP address in order to perform a cleanup.

The benefit of enabling transparency is that the clients' HTTP(S) requests can be processed and scanned by IWSVA without any client configuration changes. This is more convenient for your end users, and prevents clients from exempting themselves from security policies by simply changing their Internet connection settings.

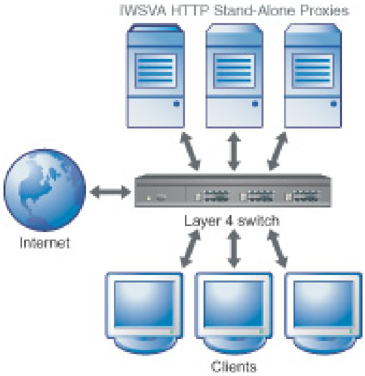


FIGURE 5-4. Forward proxy with transparency

Note: In simple transparency mode, IWSVA does not accept SSL (HTTPS) traffic. Configure the router not to redirect port 443 traffic to IWSVA.

If you configure IWSVA in simple transparency mode and the IWSVA server is connected to a layer-4 switch, you should set the HTTP listening port to 80 and enable PING on the data interface to allow users to access the Internet through IWSVA.

To configure simple transparency:

1. Click **Administration > Deployment Wizard** from the main menu.

   The Deployment Wizard displays.
2. Check **Simple Transparency mode** and click **Next**.

3. Change the **HTTP Listening port** to the same port that the Layer 4 switch is configured to use.
4. Click **Next** until the Submit button displays. Click **Submit.** Click **Close**.

Reverse Proxy

IWSVA can be used to scan content that clients upload to a Web server. When IWSVA is installed using either the forward or reverse proxy scan configuration, traffic in both directions is scanned (uploading and downloading).

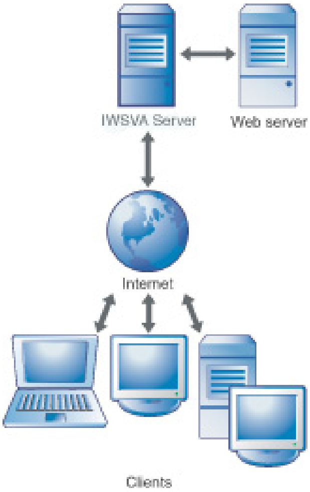


FIGURE 5-5. Reverse proxy protects Web server from clients

To configure IWSVA as a reverse proxy:

1. Click **Administration > Deployment Wizard** from the main menu.

   The Deployment Wizard displays.
2. Select **Reverse proxy** mode and click **Next**.
3. Enter the **HTTP Listening Port** number, the IP address or host name of the **Protected server.**
4. If you want to enable HTTPS access, check **Enable SSL Port** and enter the **Port Number**.

5. Click **Next** until the Submit button displays. Click **Submit.** Click **Close**.

Note: If communication with your internal Web servers is through SSL, you must configure the HTTPS port(s). For more information, see HTTPS Ports starting on page 5-17.

In reverse proxy mode, IWSVA tunnels HTTPS traffic. HTTPS decryption is not supported in Reverse Proxy Mode.

To complete your reverse proxy configuration, the IWSVA device's IP address must be registered in the DNS as the host name of the Web server that the reverse proxy is protecting. In this way, the IWSVA device appears to be the Web server, as far as the clients are concerned.

Proxy-related Settings

In addition to specifying the type of proxy configuration you want, you can also set the following parameters for the configuration:

- HTTP listening port
- Anonymous FTP logon over HTTP email address

HTTP Listening Port

If you enable HTTP scanning, be sure to specify the appropriate listening port number of a given HTTP handler so the traffic will go through.

Note: It is not necessary to configure an HTTP Listening Port in Transparent Bridge mode.

To configure the listening port number:

1. Open the IWSVA Web console and click **Administration > Deployment Wizard.**
2. Select your mode and click **Next**.
3. In the **HTTP Listening port** text box, type the port number (default values are 1344 for ICAP and 8080 for HTTP Proxy).
4. Click **Save**.

Note: IWSVA handles HTTPS connections differently from HTTP connections. Because the data is encrypted, you can configure HTTPS decryption policies to decrypt the content which can then traverse filtering and scanning policies as "normal" HTTP traffic. IWSVA examines the initial CONNECT request, and rejects it if it does not match the set parameters (such as the target URL is on the Block List or contained in the Phish pattern file, or the port number used is not defined in the `HttpsConnectACL.ini` file).

Anonymous FTP Logon Over HTTP Email Address

FTP over HTTP enables users to access hyperlinks to ftp:// URLs in Web pages and enter a URL starting with ftp:// in the address bar of their browser. If the user omits the user name when accessing this type of URL, anonymous login is used, and the user's email address is conventionally used as a password string that is passed to the FTP server.

To configure the email address to use for anonymous FTP logon over HTTP:

1. Select **Administration > Deployment Wizard Mode** from the main menu.
2. Type the **Email address to use** for an anonymous FTP log on.
3. Click **Save**.

Network Configuration and Load Handling

The number of users supported by each IWSVA instance depends on the hardware where IWSVA is installed, the average number of concurrent sessions used per user, the bandwidth used by each users' sessions, and the percentage of the user population that is using the Internet simultaneously. In general, the more powerful the IWSVA server platform, the larger IWSVA's capacity will be.

In general, a two processor dual core server with 4GB of memory and fast hard disk drives will be able to support up to 4000 users. A two processor quad core server with 8GB of memory and fast hard disk drives will be able to support up to 9500 users.

Trend Micro's general capacity planning rules make the assumption that each user opens an average of two concurrent sessions and approximately 20 percent of the user population is actively accessing the Internet.

Note: For more information on capacity sizing, refer to the IWSVA Sizing Guide.

You can install IWSVA on the network in the following modes:

- **Transparent Bridge**—Run a cable from the external (Internet-facing) network device to an IWSVA external port, and from an IWSVA internal port, to an internal network device.
- **Forward Proxy**—Run a cable from the interface configured in the CLI to the internal network device.
- **ICAP**—Connect IWSVA to the ICAP client using the interface configured in the CLI.
- **WCCP**—Trend Micro recommends using the following Cisco IOS versions when configuring WCCP with IWSVA:
  - 12.2(0) to 12.2(22). Avoid using releases 23 and above within the 12.2 family
  - 12.3(10) and above. Avoid using releases 0-9 in the 12.3 family
  - IOS 12.4(15)T3 or later should be used

After setting up the IWSVA server, open the IWSVA Web console and click **Administration > Deployment Wizard** to set the corresponding IWSVA scan mode.

Shared Policy after Registering to ARM

If you purchase Trend Micro Advanced Reporting and Management (ARM), after registering all cluster members to ARM, all members share the same policies. For more detailed information, please refer to the *Advanced Reporting and Management for InterScan Web Security Administrator's Guide*.

Note: An IWSVA cluster must have only one parent server.

You can configure the "parent"/"child" designation in the Cluster Management page or Deployment Wizard of the Web console specifies the parent node. The child node has the same policies and deployment settings, after it is synchronized with the parent.
- See more shared, cluster-level settings in Table 3-1 on page 3-8.
- To switch member roles, see To perform a manual switchover with Weighted Priority Election mode disabled: on page 3-17 or To change the weight value of a node: on page 3-20.

Configuring Internet Access Control Settings

IWSVA includes several configurations to control your clients' HTTP(S) access. These settings are separate from any scanning or URL filtering policies that you might configure for your user base.

- HTTP access can be selectively enabled for client users with a given IP address, IP range, or IP mask.
- To improve performance when client users request content from "trusted" sites, scanning, URL filtering, and URL blocking can be disabled for servers with a given IP address, or servers within a given IP range or IP mask.
- HTTP and HTTPS requests to ports or port ranges can be selectively allowed or denied for all users whose Internet access passes through IWSVA. This feature is convenient if you want to prevent certain types of Internet transfers. In addition, you can configure HTTPS decryption policies to decrypt HTTPS traffic for scanning.

Identifying Clients and Servers

For controlling client Web access or configuring servers as trusted, there are three ways to identify the client or server:

- IP address: a single IP address, for example, 123.123.123.12
- IP range: clients that fall within a contiguous range of IP addresses, for example, from 123.123.123.12 to 123.123.123.15

- IP mask: a single client within a specified subnet, for example, entering IP = 192.168.0.1 and Mask = 255.255.255.0 identifies all machines in the 192.168.0.x subnet. Alternatively, the Mask can be specified as a number of bits (0 to 32)

Client IP

In addition to the default setting that allows all clients on your network to access the IWSVA proxy, IWSVA can be configured to allow HTTP access only to those clients that you explicitly specify. If your organization does not allow everyone on your network to access the Internet, this is a convenient way to block HTTP access by default.

To allow HTTP access based on client IP:

1. Select **HTTP > Configuration > Internet Access Control** from the main menu.

   In transparent bridge mode, the destination and HTTPS ports are not available; therefore, when in this mode the **Destination Ports** and **HTTPS Ports** tabs are not present in the **Internet Access Control** screen.
2. Ensure that the **Client IP** tab is active.
3. Check **Enable HTTP Access Based On Client IP**.
4. Select the option that describes how clients are allowed HTTP access—either **IP address**, **IP range**, or **IP mask**.

   Note: If you specify a single IP address and then an IP address range containing the single IP address, the IP address range is negated if a user attempts to access a URL at the single IP address.

   For more information about identifying the clients, see Identifying Clients and Servers starting on page 5-13.

   To delete a client IP or IP range, click the corresponding **Delete** icon next to it.
5. Type a descriptive name in the **Description** field. (40 characters maximum)
6. Click **Add**.

   The client IP that you have configured is added to the list at the bottom of the **Client IP** tab. Access control settings are evaluated according to the order they appear in the list at the bottom of the **Client IP** tab.
7. Click **Save**.

Server IP White List

To maximize the performance of your network, you can configure IWSVA to skip scanning and filtering content from specific servers. For example, if you are protecting your intranet server with IWSVA in a reverse proxy configuration, you can be reasonably assured that its content is safe and you might want to consider adding your intranet servers to the Server IP White List.

After configuring the IP addresses or ranges of trusted servers, the configurations are saved to the `ServerIPWhiteList.ini` configuration file. Overlapping IP ranges are not allowed.

WARNING! **Content from servers that you configure on the Server IP white list is not scanned or filtered. Trend Micro recommends adding only those servers over which you have close control of the contents.**

In ICAP mode, the server IP white list is only applied to RESPMOD requests. REQMOD activities (such as URL filtering, Webmail upload scanning, and URL blocking) cannot be bypassed by the server IP white list for ICAP installations.

To add servers to the Server IP White List:

1. Select **HTTP > Configuration > Internet Access Control** from the main menu.
2. Ensure that **Server IP White List** tab is active.
3. Check the way you want to specify trusted servers whose content is not scanned or filtered—either **IP address**, **IP range**, or **IP mask**.

   For more information about identifying the clients, see Identifying Clients and Servers starting on page 5-13.
4. Type a descriptive name in the **Description** field. (40 characters maximum)
5. Click **Add**.

   The trusted servers that you have configured appears at the bottom of the **Server IP White List** tab.

   To delete a trusted server or range, click the corresponding **Delete** icon next to it.
6. Access control settings are evaluated according to the order they appear in the list at the bottom of the **Server IP White List** tab.
7. Click **Save**.

Destination Port Restrictions

IWSVA can restrict the destination server ports to which clients can connect. HTTP requests to a denied port are not forwarded. This approach can lock down your server and prevent clients from using services such as streaming media applications that contravene your network’s security policies by denying access to the ports used by these services.

The default post-install configuration is to deny all requests, except for those to ports 80 (HTTP), 70 (Gopher), 210 (TCP), 21 (FTP), 443 (SSL), 563 (NNTPS) and 1025 to 65535.

Note: To enable FTP over HTTP connections for clients to open FTP links in Web pages, IWSVA must be able to open a command connection to the FTP server on port 21. This requires allowing access to port 21 on the HTTP access control settings.

For a list of ports used by various applications and services, see `http://www.iana.org/assignments/port-numbers`.

To restrict the destination ports to which a client can connect:

1. Select **HTTP > Configuration > Internet Access Control** from the main menu.
2. Ensure that the **Destination Ports** tab is activated.
3. Choose the **Action** to perform. Choose **Deny** to prevent connections to a specific port or port range on a destination server, or **Allow** to permit connections to a specific port or port range.
4. Check either **Port** or **Port Range** and then enter the corresponding port(s).
5. Type a descriptive name in the **Description** field. (40 characters maximum)
6. Click **Add**. The destination port restrictions are added to the list at the bottom of the **Destination Ports** tab.

   To delete a destination port or port range to which you allow or deny access, click the **Delete** icon next to it.
7. Access control settings are evaluated according to the order they appear in the list at the bottom of the **Destination Port** tab.

   To change the order that ports appear in the list, click the up or down arrows in the **Priority** column.

8. Click **Save**.

HTTPS Ports

IWSVA can restrict which ports can be used for encrypted HTTP transactions. The default configuration is to allow only HTTPS connections on port 443 (the default HTTPS port) and 563 (the default port for encrypted news groups).

Note: If you need to access the Web console through HTTPS while connecting through IWSVA itself, allow access to the IWSVA secure console port number (8443 by default).

To restrict the ports that can be used to tunnel encrypted HTTP transactions:

1. Select **HTTP > Configuration > Internet Access Control** from the main menu.
2. Make the **HTTPS Ports** tab active.
3. Choose the **Action** to perform—either **Deny** or **Allow**.
4. Check either **Port** or **Port Range** and then enter the corresponding port(s).
5. Type a descriptive name in the **Description** field (40 characters maximum.)
6. Click **Add**. The destination port restrictions appear at the bottom of the **HTTPS Ports** tab.

   To delete any HTTPS port access restrictions that you might have configured, click the **Delete** icon next to the port or port range to remove.
7. Access control settings are evaluated according to the order they appear in the list at the bottom of the **HTTPS Ports** tab. To change the order that ports are displayed in the list, click the up or down arrows in the **Priority** column.
8. Click **Save**.

Chapter 6

Policies and User Identification Method

InterScan Web Security Virtual Appliance (IWSVA) is able to apply different HTTP virus scanning, HTTPS decryption, Applets and ActiveX security, URL filtering, IntelliTunnel, and access quota policies to different individuals or groups on your network. In this way, security policies can be customized based on your business need to handle potentially malicious code, view certain categories of Web content or to prevent the consumption of excessive bandwidth for Web browsing.

Topics in this chapter include the following:

How Policies Work

Different security settings can be configured for different users or groups on your network, based on the type of files or Internet resources they need to access. Some examples of the practical application of different security policies are the following:

- **Virus scanning:** Your organization’s acceptable user policy might generally prohibit clients from downloading audio or video files. However, there might be some groups within your company who have a legitimate business purpose for receiving these types of files. By configuring several virus scanning policies, you can apply different file blocking rules in HTTP virus scanning policies for different groups within your company.
- **Applets and ActiveX security:** To prevent clients from running applets that could intercept sensitive information and transmit it over the Internet, you might want to configure a policy for most of your company that prevents applets from connecting to their originating servers. However, if there are users in your company who have a legitimate business purpose to run these sorts of applets (for example, to get quotations through a Java applet stock price ticker), another policy could be configured and applied to a sub-set of your client base.
- **URL filtering:** To discourage your employees from engaging in non-work-related Web surfing, you might want to configure a Global Policy that blocks access to Web sites in the “gambling” category. However, you might need to configure another policy that permits access to these types of sites so your sales organization can learn more about prospects in the gaming industry. In addition to selected pre-defined categories, you can also create new Web categories to apply to URL filtering policies.
- **HTTPS decryption:** To scan encrypted content over HTTPS connections, you can configure HTTPS decryption policies based on the type of sites accessed. Once decrypted, the content can traverse through filtering and scanning policies on IWSVA as “normal” HTTP traffic. HTTPS decryption policies prevent security risks embedded in HTTPS traffic.
- **Access quotas:** IWSVA allows you to configure access quota policies to limit the volume of files that clients can download during the course of a day, week, and month, to control the amount of bandwidth that your organization uses. For those employees who have a legitimate business need to browse the Internet extensively, you can configure another policy granting them unlimited Internet access.
- IWSVA enables you to block communication provided by certain Instant Message (IM) protocols and certain authentication connection protocols.

- IWSVA provides the flexibility that allows you to configure and apply approved URL or file name lists on a per-policy bases.

In addition to being able to define custom policies that apply to specific users, IWSVA is pre-configured with two default policies, the “Global Policy” and the “Guest Policy,” to provide a baseline level of HTTP virus scanning, Applets and ActiveX security, IntelliTunnel security, and URL filtering.

Note: IWSVA supports the Guest Policy only in HTTP Forward Proxy mode with LDAP enabled.

Default Global and Guest Policies

IWSVA has default global and guest policies for the following activities: HTTPS decryption, HTTP Scan, Applets and Active X, URL Filtering, and IntelliTunnel.

- Global Policy—For all clients who access through IWSVA.
- Guest Policy—For those clients, typically temporary workers, contractors, and technicians who proxy through IWSVA using a special guest port (default port = 8081).

  The guest account is disabled by default; enable the guest account and port under **Administration > Deployment Wizard > Mode Selection > Proxy Settings** after first enabling LDAP (**HTTP > Configuration > User Identification | User Identification tab**).

Note: Guest accounts only apply to the Forward Proxy deployment mode.

By default, access quota control is not available for clients accessing IWSVA through the default listening port; which means there is no pre-configured Global Access Quota Policy.

IWSVA does not provide HTTPS decryption from guest ports. Instead, IWSVA tunnels HTTPS traffic through guest ports.

About the Guest Policy

The guest port is a feature that's available when the administrator has configured IWSVA to run in HTTP Forward Proxy mode using LDAP "User/group name authentication" as the user identification method. The administrator can opt to open the second listening port so that users who do not have accounts in an organization's directory server (for example, contract personnel or visiting vendors) can still access the Web. When IWSVA is running in HTTP Forward Proxy mode, the default port values are 8080 for user logon residing in a designated directory server configured on IWSVA, and 8081 for guest users. The Guest Policy is the only policy applied to guest users.

For more information about enabling the "User/group name authentication" user identification method, see User/Group Name Authentication starting on page 6-9.

Enabling the Guest Port

To enable Internet connectivity to network users who are not in the LDAP directory and apply guest policies, open a guest port for Web clients to communicate with IWSVA.

To enable the guest port:

1. Select **HTTP > Configuration > User Identification | User Identification** from the main menu.
2. From the **User Identification** screen, select **User/group name authentication** and then enter the designated directory server (s) of choice.
3. Click **Save**.
4. Select **Administration > Deployment Wizard** from the main menu.
5. From the **Proxy Scan Settings** screen, check "**Enable guest account**."
6. Click **Save**.

Deploying Policies

After configuring a policy, the settings are written to the database after you click **Save**. Clicking **Deploy Policies** applies the new policy configuration immediately. Otherwise, the policy changes go into effect when IWSVA reads the information from the database after the time intervals specified under **Policy Deployment Settings (in minutes)** on the **Administration > IWSVA Configuration > Policy Deployment** screen.

Note: When policies are being applied, either after the cache expiration interval or from clicking **Deploy Policies**, HTTP(S) and FTP connections are interrupted for a short time (about ten seconds).

Configuring the User Identification Method

You need to configure how IWSVA identifies clients to define the scope of HTTP virus scanning, URL filtering, Applets and ActiveX security, IntelliTunnel security, and access quota policies. Your choice of user identification method also determines how security events are traced to the affected systems in the log files and reports.

IWSVA provides three user identification methods to identify clients and apply the appropriate policy:

- IP address (default option)
- Host name (modified HTTP headers)
- User/group name authentication (LDAP)

The following table lists the different user identification method IWSVA supports in various deployment modes:

TABLE 6-1. Supported User Identification Method in Different Deployment Modes

	IP ADDRESS	HOSTNAME	USER/GROUP NAME AUTHENTICATION
Bridge Mode	Yes	Yes	Yes
Standalone/ Dependant	Yes	Yes	Yes
WCCP	Yes	Yes	Yes
Simple Transparency	Yes (if source NAT is disabled)	Yes	No
Reverse Mode	Yes	Yes	No

TABLE 6-1. Supported User Identification Method in Different Deployment Modes

	IP ADDRESS	HOSTNAME	USER/GROUP NAME AUTHENTICATION
ICAP	No	Yes	Yes

Note: For users connecting to an HTTP server with integrated Windows authentication through the IWSVA using Internet Explorer 6.0, make sure the **Use HTTP1.1 through proxy connections** option is selected in the **Tools > Internet Options >Advanced** screen for NTLM (NT LAN Manager) authentication to work properly.

IP Address

The IP address is the default identification option and requires the following:

- Client IP addresses are not dynamically assigned through DHCP as DHCP will make the IP address identification less accurate as DHCP leases expire.
- Network address translation (NAT) is not performed on the network path between the affected system and IWSVA.

If the local network meets these conditions, you can configure IWSVA to use the IP address user identification method.

When using the IP address identification method, the scope of scanning policies is defined by defining a range of IP addresses, or a specific IP address, when adding or editing a policy.

To enable the IP address user identification method:

1. Select **HTTP > Configuration > User Identification | User Identification** from the main menu.
2. From the User Identification screen, select “**IP address**.”
3. Click **Save**.

Host Name

The host name identification method requires that clients use Internet Explorer on the Windows platform. In addition to defining a policy's scope by specifying the user's host name(s) when defining accounts to which a policy applies, the **Host name (modified HTTP headers)** user identification option logs the MAC address and Windows machine name to the security event logs.

By default, only the host name portion of the host name/MAC address combination is stored in IWSVA for certain types of logs, such as the URL Access Log and reports, and is used to match policies. If you want to use both the host name and MAC address for user identification, edit `intscan.ini` and change `use_mac_address=no` to `use_mac_address=yes` in the `[user-identification]` section.

Note: Applet-filtering messages show the client IP address (and not the host name) because even when using Internet Explorer, the HTTP request is submitted by the Java plug-in, not the browser; therefore, Internet Explorer cannot add the special header to the request.

Since IWSVA is unable to obtain host name information before decrypting HTTPS contents, IWSVA does not support host name identification for HTTPS decryption policies in bridge or WCCP mode.

Host name identification relies on information included in HTTP headers by Internet Explorer. To use this identification option, you must modify the end user's Windows Registry. This modification causes the hostname of the end user's PC to be included (in encrypted format) in any HTTP request sent by Internet Explorer. IWSVA includes a utility program, `register_user_agent_header.exe`, to make this registry modification. The utility must be executed on each PC in the network—it does not need to be run again unless the hostname of the PC is changed.

You can obtain the `register_user_agent_header.exe` file from the `/usr/iwss/bin` folder on the IWSVA server or download it from following Web site:

`http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=250&regs=NABU&lang_loc=1`

Be aware of the following limitations:

- End users must be using Microsoft Windows OS.
- End users must be browsing with Internet Explorer.
- The `register_user_agent_header.exe` utility must have been executed on the end user's desktop.
- The context which executes `register_user_agent_header.exe` must have write permissions for the registry key, `HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\User Agent\Post Platform`.

To enable the Host name identification method:

1. Select **HTTP > Configuration > User Identification | User Identification** from the main menu.
2. Select **Host name (modified HTTP headers)**.
3. Click **Save**.

Note: Before your users are able to access the Internet, and for IWSVA to apply the correct policy, clients will have to run the client registration utility on each system.

Client Registration Utility

The **Host name (modified HTTP headers)** user identification option requires that you run a Trend Micro-supplied program on each Windows client before clients connect to IWSVA and access the Internet. The program file is: `register_user_agent_header.exe` and is located in the /usr/iwss/bin (IWSVA machine). An effective way to deploy this program to your clients is to invoke it from a logon script for the local Windows domain.

The program works by modifying a registry entry:

```
(HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Inter
net Settings\User Agent\Post Platform)
```

Internet Explorer includes that registry entry in the User-Agent HTTP header. You can find the identifying information logged under the **User ID** column in various log files. It alters Windows configuration values to include the MAC address of the client system and the machine name that made the HTTP requests. The MAC address is a unique and traceable identification method and the machine name is an additional and helpful identifier. For more information, refer to *Enabling MAC Address Client Identification* on page 12-56.

After running the `register_user_agent_header.exe` utility, a new registry value is created under the following key:

```
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Intern
    et Settings\User Agent\Post Platform
```

The new registry value called `IWSS25:<host_name>/<MAC address>` is encrypted, where `<host_name>` and `<MAC address>` correspond to the client that ran the utility.

User/Group Name Authentication

IWSVA can integrate with the following LDAP servers, and supports both the LDAP two and three protocols:

- Microsoft™ Active Directory for Windows Servers 2003 and 2008
- Linux™ OpenLDAP Directory 2.3.39
- Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)

LDAP Authentication Method

When you enable the "**User/group name authentication**" method, clients are required to enter their network logon credentials before accessing the Internet.

The following table shows which LDAP authentication methods can be used with each of the supported LDAP servers:

TABLE 6-2. Authentication Methods for Supported LDAP Servers

	KERBEROS	SIMPLE AUTHENTICATION	NTLM
Microsoft Active Directory for Windows Servers 2003 and 2008	yes	yes	yes
Linux OpenLDAP 2.3.39	yes	yes	no

TABLE 6-2. Authentication Methods for Supported LDAP Servers (Continued)

	KERBEROS	SIMPLE AUTHENTICATION	NTLM
Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)	no	yes	no

Note: To use the Digest-MD5 authentication method with the Sun Java System Directory Server 5.2, all passwords must be stored as clear text in the LDAP directory.

Choose **Simple** from the **LDAP Authentication Method** area of the **User Identification** page (**HTTP > Configuration > User Identification| User Identification**) to have IWSVA send the user's credentials (used in the Admin account) as plain text for the initial LDAP connection only.

For increased security protection, IWSVA uses the advanced authentication method (Kerberos or Digest-MD5) for all subsequent user logon authentications from IWSVA to the LDAP server. In addition, IWSVA still validates user credential using Kerberos authentication method even when you select simple authentication on the LDAP server.

Transparent Identification

Transparent Identification uses several authentication mechanisms to reduce the number of times the user must authenticate to access the Internet. It combines domain-level authentication and the Windows client polling activities into one transparent operation to discover the user credentials and to eliminate the need to manually enter authentication credentials.

Using Transparent Identification, IWSVA:

- Parses the events in the security log on the Active Directory server to obtain the IP-user mapping relationship
- Retrieves Windows client's active user and domain name
- Uses the fetched information to match with policies to reduce the pop-up authentication window as much as possible

If the transparent identification query fails, IWSVA leverages the existing proxy- and browser-based LDAP authentication methods. See *Figure 6-1*.

For more information on Transparent Identification, see Configuring LDAP Settings on page 6-16 and Best Practices for IWSVA on page E-1.

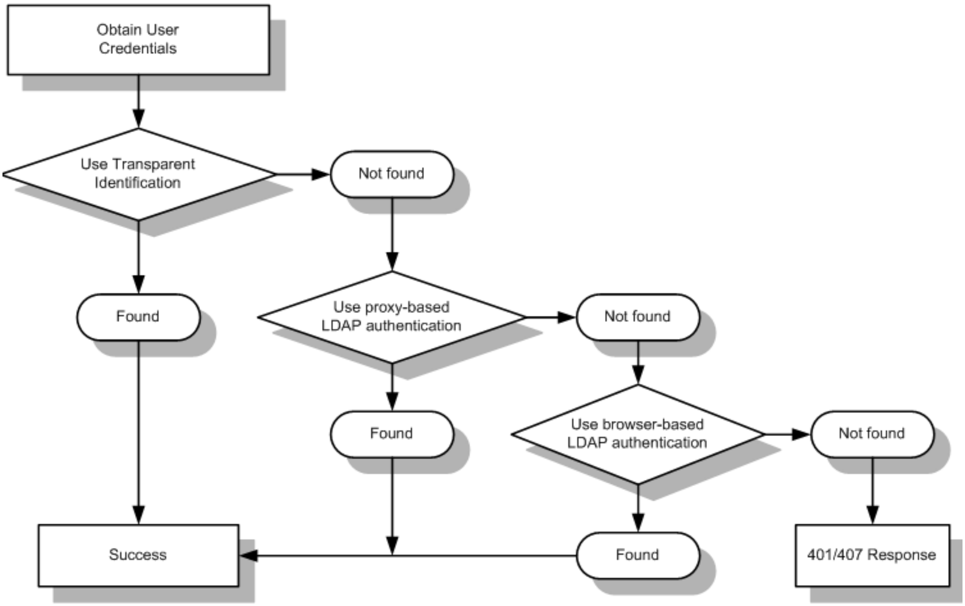

Obtain User Credentials
Use Transparent Identification
Not found
Found
Use proxy-based LDAP authentication
Not found
Found
Use browser-based LDAP authentication
Not found
Found
Success
401/407 Response

FIGURE 6-1. Transparent Identification Flow

Note: The following exceptions apply to Transparent Identification:
- The Transparent Identification solution only applies to Windows AD 2003 and 2008 environments.
- Login names using the "%" special character are not supported when the Window Client Query is enabled.
- Login names using the "$" special character are not supported when Domain Controller query is enabled.
- Transparent Identification cannot distinguish the correct user when:
- - More than one user accesses a shared PC with different logon accounts or
- - The same user logs into a single machine with the same credentials to activate multiple sessions.

Transparent identification solution applies to the following client platforms:

- Windows 2000
- Windows 2003
- Windows XP
- Windows Vista
- Windows 7
- Windows 2008

Transparent identification applies to all deployment modes that support Active Directory (AD) authentication.

LDAP Communication Flows

When clients request Internet content, they are prompted to enter their network credentials. Simple authentication sends the network credentials through clear text. Advanced authentication uses a Kerberos server as a central secure password store. Therefore, the benefit of using Kerberos is that it provides a higher degree of security.

After the client's credentials are authenticated with a Kerberos Server, a special encrypted "ticket" certified by the Kerberos server is used to access IWSVA and the Internet.

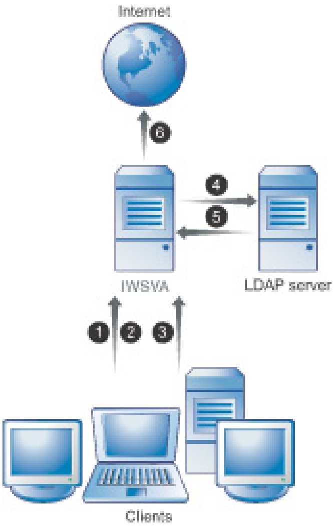


FIGURE 6-2. LDAP Communication Flow Using Kerberos Authentication

When User/group authentication is enabled in either forward proxy mode or transparent mode with Active Directory, you can take advantage of the automatic authentication feature provided in the Internet Explorer Web browser. With automatic authentication, clients already logged on the domain network can access the local Intranet without having to enter the logon information (such as the user name and password); that is, no password pop-up screen displays.

Note: You must configure IE settings to enable automatic authentication on each client computer. By default, automatic authentication is enabled in IE 7.0.

IWSVA supports Internet Explorer automatic authentication for the following authentication method:

- Single domain (LAN or 802.11)
- Global catalog enabled in a multi-domain environment (LAN or 802.11)

To enable automatic authentication in IE:

1. Open Internet Explorer on a client computer, click **Tools > Internet Options** and then click the **Security** tab.
2. Click **Local intranet** and click **Custom level. . .**
3. Select **Automatic logon only in Intranet zone** and click **OK**.
4. Click **Site**, select **Automatically detect intranet network**, and click **Advanced**.
5. In the Intranet Network screen, type the IWSVA hostname and click **Add**.
6. Save the settings.

To enable automatic authentication in Firefox:

1. Open Firefox on a client computer and type "about:config" in the address field.
2. Type "ntlm" in the **Filter** field.
3. Double-click **network.automatic-ntlm-auth.trusted-uris**.
4. A pop-up screen displays. Type the hostname of the IWSVA server and click **OK**.

Note: For other supported Web browsers and authentication methods not listed above, users will need to type the logon information in a pop-up screen.

Note: Trend Micro recommends that you use global catalog instead of referral chasing. If you enable referral chasing, automatic authentication may not work for users whose information is not found in the main LDAP server. In this case, a Web browser window displays for these users to type their logon information.

LDAP Authentication in Transparent Mode

Before configuring LDAP authentication on IWSVA deployed in transparent mode (bridge and WCCP), review the following criteria to ensure each item is fully met.

- A valid hostname must be assigned in the Deployment Wizard when configuring Transparent Bridge or WCCP modes. The same hostname must also be entered in the corporate DNS server.

- Ensure that the user ID cache is enabled, which is the default setting. This setting must be enabled before enabling transparent mode authentication. You can enable user ID cache using the `configure module ldap ipuser_cache enable` command in the CLI.
- By default, IWSVA keeps user ID cache information for up to 1.5 hours. If you need to lower the cache timeout value, use the `configure module ldap ipuser_cache <interval>` command in the CLI to set a shorter cache interval.
- If authentication is enabled, IWSVA will block all non-browser applications trying to access the Internet. For example, the MSN application may try to access the Internet before the user has a chance to log in the IWSVA server. If this happens, the application will be blocked as the user has not successfully authenticated to IWSVA. You can perform one of the following:

  a. Enable the Domain Controller or Windows client query. After enabling either of these options, no authentication is required because IWSVA obtains the username and domain name through domain controller or client query.

  b. Bypass LDAP authentication for the application by adding the URLs that application accesses to "Global Trusted URLs." The URLs in this list will bypass both authentication and content scanning.

  c. Instruct users to open their Web browsers and get authenticated before starting up applications that need Internet access.

  d. Add the IP address of the client machine to "LDAP authentication White List." IP address in this list will bypass LDAP authentication.

- When User/group authentication is enabled in either forward proxy mode or transparent mode with Active Directory, you can take advantage of the automatic authentication feature provided in the Internet Explorer Web browser. With automatic authentication, clients already logged on to the domain network can access the local Intranet without having to enter the logon information (such as the user name and password); that is, no password pop-up screen displays.

Note: You must configure your IE settings to enable automatic authentication on each client computer. By default, automatic authentication is enabled in IE 7.0.

Configuring LDAP Settings

If you want to use LDAP user/group names for authentication and policy configuration purposes, you must set IWSVA's user identification feature to use your corporate LDAP server.

Note: If you want to apply the Guest Policy for those network users who are not in your LDAP directory, enable the guest account and configure the guest port (default = 8081) that receives those requests on the IWSVA device. For more information about enabling the guest account and configuring the guest port, see Enabling the Guest Port starting on page 6-4. If the guest port is not enabled, only users in the LDAP directory can browse the Internet.

To configure IWSVA to use the user/group name authentication method:

1. Select **HTTP > Configuration > User Identification | User Identification tab** from the main menu.
2. Under the **User Identification Method** section, check **User/group name authorization**.
3. Under the User/group Authentication Settings section in the LDAP Settings section, click the **Select LDAP vendor** link.
4. In the secondary browser window, select from the list of supported LDAP servers the LDAP vendor that you are using.

   Note: In case future versions of Microsoft Active Directory modify the schema, IWSVA supports changing the attribute names that make up a user's distinguished name. If you're using either Microsoft Active Directory 2003 or 2008, you should select the **Default settings** option.

5. In the **Configure LDAP Connection** secondary window, click **Save** to confirm your LDAP vendor choice.
6. On the **User Identification** configuration screen, in the **LDAP Settings** section, enter the **LDAP server hostname** using the Fully Qualified Domain Name (FQDN).

Entering the LDAP server hostname's IP address is also acceptable, but FQDN format is recommended due to an incompatibility between Kerberos servers and identifying LDAP servers using their IP address.

7. Enter the **Listening port number** used by the LDAP server that you have chosen (default = 389). If your network has multiple Active Directory servers and you have enabled the Global Catalog (GC) port, change the listening port to 3268.

Note: If you enable the Global Catalog in Active Directory, you might need to configure your firewall to allow communication through port 3268.

8. Enter the "**Admin account**" and **Password** for a credential with at least read authority to the LDAP server. If the domain is *us.example.com*:

   - For Microsoft Active Directory, use the UserPrincipalName for the admin account, for example, *NT_Logon_ID@us.example.com*.
   - For OpenLDAP and the Sun Java System Directory Server 5.2, enter the Distinguished Name (DN) for the admin account (for example, *uid=LOGON_ID,ou=People,dc=us,dc=example,dc=com*).

9. Enter the **Base distinguished name** to specify from which level of the directory tree you want IWSVA to begin LDAP searches.

   The base DN is derived from the company's DNS domain components; for example, LDAP server `us.example.com` would be entered as *DC=example, DC=com*.

   If you are using Active Directory servers with the Global Catalog (GC) port enabled, use the root domain of the Global Catalog-enabled Active Directory; for example, use *dc=example,dc=com*.

10. Select the LDAP authentication method to use—either **Simple** or **Advanced**.

    If you opt for **Advanced** authentication, the following authentication methods are used:

    - Microsoft Active Directory and OpenLDAP: Kerberos
    - Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server): Digest-MD5

Additionally, configure the following parameters to use Advanced authentication:

- Default Realm
- Default Domain
- **KDC and Admin Server:** The hostname of the Kerberos key distribution server. If you are using Active Directory, this is typically the same host name as your Active Directory server.
- **KDC port number:** Default port = 88

  When using NTLM to authenticate with KDC(s) on a different forest through Internet Explorer or using IWSVA to do referral chasing with Active Directory, Trend Micro recommends enabling "Use HTTP 1.1 through proxy connections." This setting can be found on the Internet Explorer **Tools** menu **> Internet Options > Advanced** tab. Enabling this setting prevents Internet Explorer from cutting off the "Keep-Alive connection" setting. Note that using NTLM is only supported with Microsoft Active Directory.

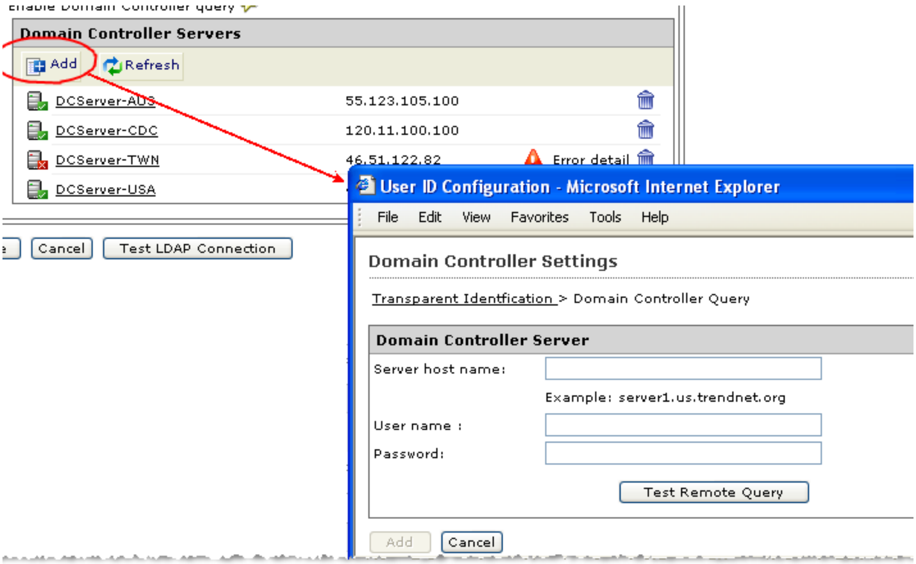
11. If a client cannot authenticate using the LDAP and/or Kerberos server that you specify, you can configure IWSVA to check other LDAP and/or Kerberos servers on your network. Check the **Enable Referral Chasing** check box and then click the **Primary referral server** and **Secondary referral server** links.

12. To enable Transparent Identification, you can click the check box for **Enable Windows client query**, **Enable Domain Controller query**, or both. Both functions require domain administrator privileges (belonging to the "Domain Admins" group) and use the account information entered in Step 8 on page 6-17.)

Note: Before enabling the Windows client query, you must:
- Belong to a local administrator's group (Domain Admins) of all windows clients in your organization.
- Verify that Windows Management Instrumentation (WMI) service (or the domain controller query) has started in all windows clients, and that it can be accessed through WMI query (by enabling 'remote administration' in the Windows firewall or enabling port 135 and related dynamically-assigned WMI communication ports on other firewall products.)
- If transparent identification is enabled, you should enter the account of the Domain Administrator's group in the Active Directory server.

- Enabling Windows client query allows IWSVA to obtain the user name and domain name transparently. Click the **Test Client** link to test the client connection and troubleshoot.

Note: Any client with a firewall blocking the necessary ports, 135 and 2201, will prevent IWSVA from polling the client PCs and obtaining information. Admins should create firewall policies that allow access to the client for these two ports from the IWSVA IP address.



Enable Domain Controller query

Domain Controller Servers

DCServer-AUS	55.123.105.100	
DCServer-CDC	120.11.100.100	
DCServer-TWN	46.51.122.82	Error detail
DCServer-USA		

User ID Configuration - Microsoft Internet Explorer

Domain Controller Settings

Transparent Identfication > Domain Controller Query

Domain Controller Server

Server host name:

Example: server1.us.trendnet.org

User name :

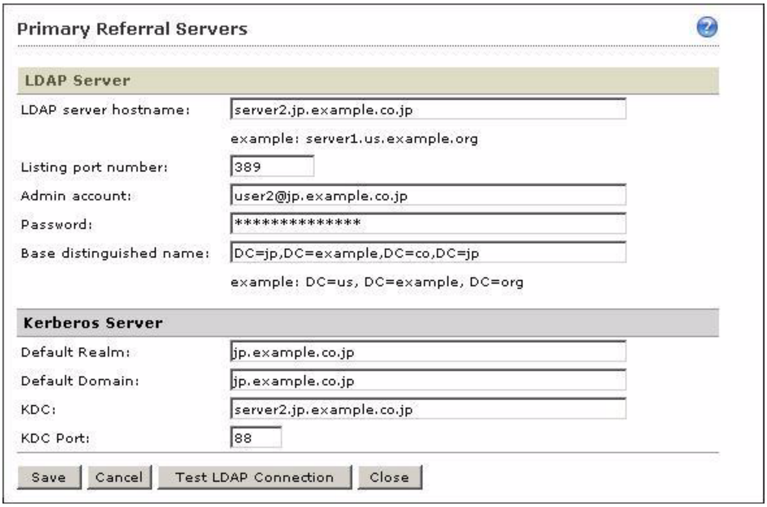
Password:

FIGURE 6-3. Enabling the Domain Controller Query

- Enabling the Domain Controller query allows IWSVA to receive the event logs for the domain controllers in the list and to parse it for user information. When first enabled, users receive a prompt to add the Domain Controller server(s) or to refresh the list of Domain Controller servers. If new Domain Controller servers are not auto-detected, they can be added manually by clicking Add in a secondary window. After adding information, click **Test Remote Query** to verify the Domain Controller server connection. All Domain Controller servers added in the configuration file can have IWSVA query the event logs for username and IP address information. (See *Figure 6-3*.)

13. Enter the information for the other LDAP servers.

Note: If you are using Active Directory servers and have enabled the Global Catalog port (default = 3268), then IWSVA referral chasing configurations are not supported. IWSVA uses a different mechanism to query Active Directory servers when the Global Catalog port is enabled, thus configuring referral servers is redundant.



Primary Referral Servers

LDAP Server

LDAP server hostname:	server2.jp.example.co.jp example: server1.us.example.org
Listing port number:	389
Admin account:	user2@jp.example.co.jp
Password:	**************
Base distinguished name:	DC=jp,DC=example,DC=co,DC=jp example: DC=us, DC=example, DC=org

Kerberos Server

Default Realm:	jp.example.co.jp
Default Domain:	jp.example.co.jp
KDC:	server2.jp.example.co.jp
KDC Port:	88

FIGURE 6-4. Configure referral servers

14. Configure the **LDAP Authentication White List** to exempt hosts from the LDAP authentication process.

For example, if you have an application server that access the Internet and you want to permit its access without requiring the server to authenticate, you can include the server's IP address in the LDAP authentication white list.

IWSVA will only apply IP address-based policy settings and bypass user/group name checking.

15. To verify the information has been entered correctly and IWSVA can communicate with the LDAP servers that you configured, click **Test LDAP Connection** on the **User Identification** page.

    A message appears, indicating that you have successfully contacted the LDAP server.

16. Click **Save**.

LDAP Query Matching Across Main and Referral Servers

When adding users or groups to a policy's scope using the "User/group name authentication" identification method, IWSVA initially searches the main LDAP server. If no matching entries are found, the search is extended to the Primary Referral Server and the Secondary Referral Server. However, if entries matching the search string are found in the main LDAP server, the query will not return matches in the Primary and Secondary Referral servers.

For example, assume the following:

- Main LDAP server contains entries "John Smith" and "John Jones"
- Primary referral server contains entry "John Watson"
- Secondary referral server contains "John Carter Rubin"

A query for "John" only returns "John Smith" and "John Jones" because matching entries exist in the main LDAP server and the search will not extend to the referral servers. However, a query for "John Carter" extends down to the secondary referral server and return "John Carter Rubin" because no matching entries exist in the main or primary referral servers.

Note: Since the 'member' attribute is incomplete in some built-in groups that exist in Active Directory (such as 'Domain Users'), IWSVA will not be able to obtain membership information for these groups through LDAP search. Trend Micro recommends you create policies based on user-defined groups instead of built-in groups.

Cross Domain Active Directory Object Queries

Trend Micro recommends using the Global Catalog port (3268) as the IWSVA LDAP communication port when using Microsoft Active Directory. Using port 3268 enables cross domain group nesting object queries. This applies when an object's attribute on one domain refers to another object residing on a different domain (for example, cross-domain user or group membership that resides on different domains in a forest).

For retrieving cross-domain group object attribute(s), you must create groups with the "Universal" Group Scope to ensure that cross-domain group memberships within an Active Directory forest are included in the Global Catalog. Using the Universal Group Scope to create groups also allows cross-domain queries. Avoid creating or using Global Group policies when the Global Catalog has been enabled.

Note: To configure IWSVA to listen on port 3268, the Microsoft Active Directory server that IWSVA uses should have the Global Catalog enabled.

Since the member attribute is not replicated to the Global Catalog for all group types, and because the *memberOf* attribute derives its value by referencing the member attribute (called back links and forward links, respectively), search results for members of groups, and groups in which a member belongs, can vary. Search results depend on whether you search the Global Catalog (port 3268) or the domain (port 389), the kind of groups that the user belongs to (global groups or domain local groups), and whether the user belongs to universal groups outside the local domain.

For more information, search for the article "How the Global Catalog Works" at http://www.microsoft.com.

Configuring the Scope of a Policy

Whether configuring HTTPS decryption, HTTP virus scanning, Applets and ActiveX security, URL filtering, IntelliTunnel security, or access quota policies, the first step is the same—to configure the policy's scope by identifying the client users to which the policy applies. The following three procedures describe how to select the accounts using the IP address, Host name (modified HTTP headers) and the User/group name authentication user identification methods. Those procedures are:

- Configuring Policies Using IP Addresses on page 6-23
- Configuring Policies Using Host Names on page 6-24

- Configuring Policies Using LDAP on page 6-24

Note: Even if you configure IWSVA to use the Host name (modified HTTP headers) or User/group name authentication user identification method, you can always specify clients by entering an IP address or IP address range.

Before adding a policy and configuring its scope, set the user identification method. See Configuring the User Identification Method starting on page 6-5 for more information.

Configuring Policies Using IP Addresses

Configuring policies using the clients' IP addresses is the simplest identification method and is always available, regardless of the user identification method you have configured to use.

To configure a policy's scope using the IP address user identification method:

1. From the main menu, click **HTTP** and choose the type of policy to create (**HTTPS Decryption policies**, **HTTP Scan Policies**, **Applets and ActiveX Policies**, **URL Filtering Policies**, **IntelliTunnel Policies**, or **Access Quota Policies**).
2. In the screen that corresponds to the type of policy selected, click **Add**.
3. Type a descriptive **Policy name**.

   Policy names that include references to the users or groups to which they apply (for example, "Virus Policy for Engineers" or "URL Filtering Policy for Researchers") are easily recognizable.
4. Select the users to which this policy applies by typing the upper and lower bounds of a contiguous range of IP addresses in the **From** and **To** fields. Alternatively, type a single **IP address**. Click the corresponding **Add** button to add the addresses to the policy.
5. When you have named your new policy and defined the IP address(es) to which it applies, click **Next** to proceed with the other policy settings.

Configuring Policies Using Host Names

All clients must run a Trend Micro-supplied utility before clients are subject to a policy that uses the host name (modified HTTP headers) identification method. For more information, see Client Registration Utility starting on page 6-8.

To configure a policy's scope using the client host names:

1. From the main menu, click **HTTP** and then choose the type of policy to create (**HTTPS decryption**, **HTTP Scan Policies**, **Applets and ActiveX Policies**, **URL Filtering Policies**, **IntelliTunnel Policies**, **Access Quota Policies**).
2. In the screen that corresponds to the type of policy that you selected, click **Add**.
3. Type a descriptive **Policy name**.
4. Select the users to which this policy applies by typing the **Host name** of the client and clicking **Add**.

   Repeat typing the host names and clicking **Add** until the Type/Identification table on the right side of the screen shows all the clients to which the policy applies.
5. When you have named your new policy and defined the account(s) to which it applies, click **Next** to proceed with configuring the rest of the policy.

Configuring Policies Using LDAP

Before configuring a policy using users or groups from your LDAP server, set the user identification method and enter the details of your LDAP server. For more information, see Configuring LDAP Settings starting on page 6-16.

To configure a policy's scope using users and groups from an LDAP server:

1. From the main menu, click **HTTP** and then choose the type of policy to create (**HTTPS decryption**, **HTTP Scan Policies**, **Applets and ActiveX Policies**, **URL Filtering Policies**, **IntelliTunnel Policies**, **Access Quota Policies**).
2. In the screen that corresponds to the type of policy that you selected, click **Add**.
3. Type a descriptive **Policy name**.
4. To query your LDAP directory for users or groups to add to your policy:
   a. Check either **User** or **Group**.
   b. Type the first part of the user or group name in the **Name** field and click **Search**.

   c. When the list box displays users or groups that match your search criteria, highlight the user or group to add to the policy and click **Add**.

5. Repeat adding users or groups until your policy's scope is complete.
6. When you have named your new policy and defined the account(s) to which it applies, click **Next** and proceed with configuring the rest of the policy.
7. Configure the referral servers if the user credential exists on a different directory server other than the one configured.

   This is an exception that exists if IWSVA is configured to use the Global Catalog port 3268 for Microsoft AD, where referral server configurations do not apply.

Login Accounts

Up to 128 users can access IWSVA using assigned access rights. When in the application, users can make configuration changes that are recorded in the audit log (see Audit Log on page 12-24).

If you have a team of security administrators who are responsible for different functions and who might also have help desk privileges, then assigning them access rights can be beneficial to your organization. To manage IWSVA, these users can have different logon credentials with different privileges.

Access rights can also give you the ability to audit what is being changed in IWSVA. If you have the need to comply with certain government agency standards, then this function can be critical.

About Access Rights

There are three levels of access:

- Administrator—Users have complete and unrestricted access to the system. They can read and modify any settings accessible through the console, including creating, deleting, and modifying user accounts. Administrator can use this account and password to log into the CLI. This is the default access for new users.
- Auditor—Users cannot make any configuration changes; they can view configurations, logs, and reports. They can also change their passwords.

- Reports only—Users can only view the Summary pages and scheduled reports. They can generate logs and real-time report queries and change their own password.

Note: Accounts that have administrator privileges can log in to the terminal console through SSH.

Adding a Login Account

To add a login account:

1. From the main menu, click **Administration > Management Console > Account Administration**.
2. In the Account Administration screen, click **Add**.
3. In the **Login Accounts** page, complete the necessary information:
   - Username—The name of the user assigned to the login account.
   - Password—Should be a mixture of alphanumeric characters between 4 and 32 characters long. Avoid dictionary words, names, and dates.
   - Description—The field that briefly describes the login account.
   - Access Rights—See About Access Rights starting on page 6-25.
4. Click **Save**.

   The new login account appears in the **Account Administration** screen.

Changing a Login Account

To change a login account:

1. From the main menu, click **Administration > Management Console > Account Administration**.
2. Click on the desired username.
3. In the Login Accounts screen, change the necessary information:
   - Username—The name of the user assigned to the login account.
   - Password—Should be a mixture of alphanumeric characters between 4 and 32 characters long. Avoid dictionary words, names, and dates.
   - Description—The field that briefly describes the login account.
   - Access Rights—See About Access Rights starting on page 6-25.

4. Click **Save**.

   The changed login account appears in the **Login Accounts** screen.

Note: If an administrator account logs into the terminal console through SSH, and does not close the session, the administrator cannot modify the account directly to "Auditor" or "Reports only." A warning message will appear.

Chapter 7

Configuring HTTP Scanning

This chapter describes how to configure HTTPS decryption, HTTP virus scanning, and applets and ActiveX security policies in InterScan Web Security Virtual Appliance (IWSVA). Topics in this chapter include:

Enabling HTTP Scanning and Applets and ActiveX Security

You can enable or disable HTTP scanning from the Summary page of the Trend Micro™ InterScan™ Web Security Virtual Appliance (IWSVA) Web console.

Note: In addition to enabling HTTP scanning and Applet/ActiveX security, ensure that HTTP traffic is turned on, otherwise clients cannot access the Internet. (See Enabling the HTTP(s) Traffic Flow starting on page 5-2.)

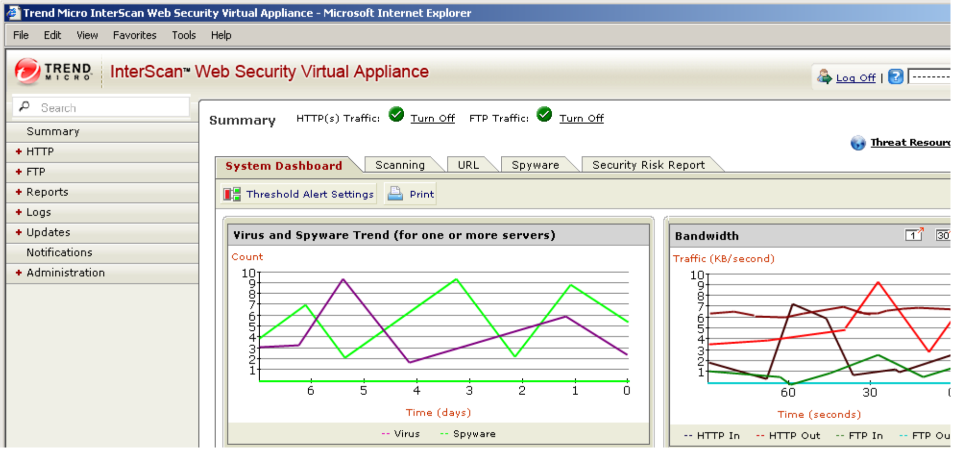


FIGURE 7-1. Summary page

To enable HTTP scanning and Applets and ActiveX Security:

1. Open the IWSVA Web console and click **Summary** in the left-hand column.
2. If **HTTP(s) Traffic:** is shown as a red circle with a white “x”, click the adjacent **Turn On** link to start the IWSVA HTTP proxy daemon.
3. Go to **HTTP > HTTP Scan > Policies**.
4. At the top of the page, check **Enable virus scanning** and **Enable Web reputation**, then click **Save**.

5. Go to **HTTP > Applets and ActiveX** > **Policies**.
6. At the top of the page, check **Enable Applet/ActiveX security**, then click **Save**.

HTTP Scanning Performance Considerations

There are trade-offs between performance and security while scanning HTTP traffic for malicious content. When users click a link on a Web site, they expect a quick response. This response, however, might take longer as gateway antivirus software performs virus scanning. Some of the requested files might be large, and determining whether the file is safe requires downloading the entire file before it is relayed to the user. Content might also consist of many small files. In this case, the user's wait is the result of the cumulative time needed to scan the files.

One way to improve the user's experience is to skip scanning large files or files that are not likely to harbor viruses. For example, you can skip all files with an extension of `.gif`, or all files with a MIME type.

When configured to skip scanning a file because of its MIME content-type, IWSVA attempts to determine the file's true-file type and match it to the claimed MIME type before skipping it. If the file's true-file type maps to a different MIME type than indicated in the Content-type header attached to the transaction, the file is scanned. Unfortunately, there is not always a clear mapping between file types and MIME types. If IWSVA cannot map the true-file type to a MIME type, it is skipped according to the Content-type header as configured.

You can exclude files from scanning based on the file extension. Trend Micro recommends that you minimize the list of MIME content-types to skip. In general, relying on the scan engine to determine whether a file should be scanned is safer than trying to pick out which file types you want to skip yourself. First, the content-type HTTP header might not accurately represent the true type of the content to download. Second, some types that you might think are safe to skip (for example, text) might not really be safe (because scripts are text, and might possibly be malicious). One more area where you might want to use MIME content-type skipping is where you are consciously making a trade-off in safety versus performance. For example, a lot of Web traffic is text, and the IWSVA scan engine scans all that traffic because the content might contain scripts, which are potentially malicious. But if you are confident that you are browsing an environment that cannot be exploited by Web scripts, you might choose to add text/* to your MIME content-type skip list so IWSVA does not scan Web pages.

Malicious code within a small file can quickly spread throughout a network. Malicious code that requires a large file for transport propagates more slowly, because the file containing malicious code takes longer to transmit. Therefore, it is important to screen small files efficiently and completely.

Note: System performance may be adversely affected if the main policy for ActiveX scanning directs all PE (windows executable) files to be scanned (not just COM objects, of which ActiveX controls are a subtype), or if all unsigned PE files are to be blocked. The performance impact occurs because the Javascan daemon—which enforces policy for these files—as well as Java Applets) is invoked more often.

HTTPS Security

HTTPS (Hypertext Transfer Protocol with Security) is a combination of HTTP with a network security protocol (such as SSL, Secured Sockets Layer). HTTPS connection is used for Web applications (such as online banking) that require secured connections to protect sensitive content. Since traditional security devices are unable to decrypt and inspect this content, virus/malware and other threats embedded in HTTPS traffic can pass unobstructed through your security defenses and on to your enterprise network.

IWSVA supports HTTPS decryption and scanning in the following modes:

- Transparent bridge
- WCCP
- Forward proxy

Dangers of Unchecked HTTPS Content

The following lists some major concerns about HTTPS connections:

- Virus scanning and content filtering policies cannot be applied to encrypted data
- Digital certificates can be forged, expired or revoked since clients rarely check the certificate revocation list
- Legitimate certificates can be easily obtained by a malicious third-party, causing users to assume that the information they provide is secure

- Web browsers are vulnerable to certificate insertion attacks that allows a malicious intruder to gain access to a corporate intranet
- Users may not have the required knowledge to decide if a certificate is to be trusted
- Monitoring HTTPS traffic is difficult since the URL path and other information are concealed

SSL Handshake Overview

To use the SSL protocol to establish an HTTPS connection, a Web server needs to install an SSL certificate. Certificates are supplied by a Certificate Authority (CA) and helps determine that a Web site is trustworthy, sensitive information (such as credit card numbers) is encrypted, and data transmitted cannot be tampered with and forged.

When a client initiates an SSL session by typing a URL that starts with https:// instead of http://, an SSL handshake is performed to verify identification (such as certificate exchange and validation) and process encryption methods required for the session. The IWSVA server acts as an intermediary between a client and a secure Web server to validate server certificates. The following describes a simplified SSL handshake process:

1. The client Web browser sends a connection request and its encryption data to the Web server. IWSVA forwards the request to the Web server.
2. The Web server returns its SSL information (including the server certificate). IWSVA checks the server certificate.
3. If the server certificate passes validation tests, the HTTPS connection is allowed between the Web server and the client. IWSVA applies HTTPS decryption policies to scan encrypted content.

   If the Web server requests a client certificate, IWSVA either blocks or tunnels the encrypted traffic.

For more information on server certificate management, refer to Managing Digital Certificates on page 7-62.

HTTPS Decryption and Process Flow in IWSVA

After an HTTPS connection is allowed between the Web server and the client, IWSVA closes the HTTPS security loophole by decrypting and inspecting encrypted content. You can define policies to decrypt HTTPS traffic from selected Web categories. While decrypted, data is treated the same way as HTTP traffic to which URL filtering and scanning rules can be applied.

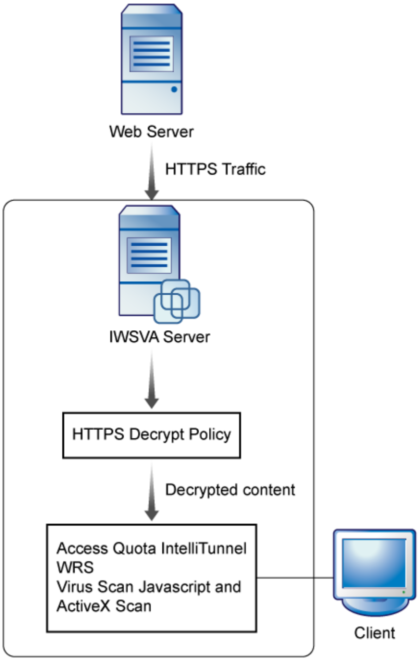


FIGURE 7-2. Decrypted HTTPS traffic flow in IWSVA

The HTTPS decryption feature offers the following benefits:

- Decryption at the gateway—IWSVA is able to decrypt HTTPS traffic and apply existing security policies.

- Data privacy is preserved—Decrypted data is completely secure since it is still in the IWSVA server's memory. Before leaving the IWSVA server, the data is encrypted for secure passage to the client's browser.
- Central certificate handling—IWSVA verifies certificates issued by remote servers and manage certificates to relieve clients of the critical tasks.

Configuring HTTPS Decryption Policies

Before IWSVA can apply scanning and filtering policies on encrypted content, you must configure HTTPS decryption policies to decrypt the content. Similar to the way you configure URL filtering policies, you configure HTTPS encryption policies to decrypt content based on selected Web categories. For example, you can configure an HTTPS decryption policy to decrypt encrypted content from Web sites in the Business categories.

HTTPS decryption and URL filtering policies use the same Web category grouping and naming. You can also configure custom categories to meet the needs of your company or users.

Note: IWSVA only matches the first custom category regardless of whether zero or more than one custom category is selected.

In bridge mode, if a proxy server is located between IWSVA and the Web server and client browsers are configured to access the Internet through the proxy server, IWSVA tunnels or decrypts and scans HTTPS connections based on the policy settings.

HTTPS Accelerator Card Support

For customers that have more than 20-25 percent of HTTPS traffic, IWSVA has drivers that support HTTPS accelerator cards, which can be used for the demanding computational calculations needed for HTTPS and save the general purpose CPU cycles for other IWSVA functions– such as content inspection. The accelerator card is designed to offload the CPU intensive operations of SSL key pair negotiation, decryption of the HTTPS stream for content inspection, and re-encryption of the content for secure delivery to the client workstation.

IWSVA supports two types of Silicom cards:

- PCI-E 61
- PCI-X 51

Using the accelerator card allows systems to offload high-level SSL or IPsec protocol commands that reduce the host I/O traffic and system processor to increase the total system throughput. This also frees system processor resources for other functions, increasing overall system performance.

Creating a New HTTPS Decryption Policy

Creating a new HTTPS decryption policy is a three-step process:

- Select the accounts to which the policy applies
- Specify the Web site categories whose traffic you want to decrypt
- Select an exception list

To create a new HTTPS decryption policy:

1. Open the IWSVA Web console and click **HTTP > HTTPS Decryption > Policies** from the main menu.

Click **Add**. The **HTTPS Decryption Policy: Add Policy** screen appears.

2. Type a descriptive **Policy name**.

Policy names that include references to the users or groups to which they apply, for example, "HTTPS decryption policy for Web Mail," is easy to remember.

3. Select the users to which the policy applies.

The options on this page depend upon the user identification method that you are using—either *IP address*, *Host name (modified HTTP headers),* or *User/group name authentication (LDAP)*. For more information about configuring the user identification method and defining the scope of a policy, see Configuring the User Identification Method starting on page 6-5.

4. Click **Next**.

5. On the **Specify Categories** screen, ensure that **Enable policy** is selected.

6. Select the URL categories to decrypt.

To select all the categories of a group, click **Select All** for the group. The group does not need to be expanded for you to select all categories in a group.

7. Type an optional **Note** to include useful information about this policy for future reference.
8. Click **Next**.
9. If you want to apply an exception list, in the **Specify Exception Lists** screen, select an approved URL list name from the drop down list box. IWSVA tunnels HTTPS traffic from a URL in the exception list; that is, the encrypted content will not be decrypted for inspection.
10. Click **Save**.
11. In the **HTTPS Decryption Policies** screen, set the priority of the new policy (under the **Priority** column) by clicking the up or down arrow.

    The **Priority** setting determines which policy is applied if there are accounts belonging to two or more policies.
12. Click **Save**.
13. To immediately apply the policy, click **Deploy Policies**; otherwise, the policy is applied after the database cache expires.

WARNING! **In proxy mode, IWSVA applies HTTPS decryption policies based on the client's browser domain. However in transparency mode, since IWSVA is unable to obtain client domain information, IWSVA applies HTTPS decryption policies to the CommonName in the server certificate.**

HTTPS Decryption Settings

Click **HTTP > HTTPS Decryption > Settings** to configure the following:

- Server certificate validation
- Client certificate handling
- CA certificate import/export

Server Certificate Validation

In the Server Certificate Validation screen, enable server certificate validation and configure validation settings to automate certificate tests such as querying certificate revocation list and establishing certificate validity.

Note: If you disable certificate validation, clients can access any HTTPS Web sites without checking server certificates.

If a certificate does not pass a certificate validation test, clients can still choose to access a Web site through HTTPS connection. A warning screen displays on the client's browser.

To configure server certificate validation:

1. From the main menu, click **HTTP > HTTPS Decryption > Settings**. The Server Certificate Validation screen displays.
2. Select **Enable Certificate Verification** to check server certificates.
3. Select one or more of the following options:
   - **Deny Certificates where the CommonName does not match the URL**—Select this option to deny a certificate if the CommonName does match the accessed URL. IWSVA treats the certificate as invalid.
   - **Allow Wildcard-Certificates**—Select this option to allow and verify certificates whose CommonName is represented by a wildcard. Disable this option to deny any certificate with a CommonName expressed using wildcards.
   - **Deny expired or wrong purpose certificates**—Select this option to deny certificates that are expired or certificates that cannot be used for the intended purpose.
   - **Verify entire certificate chain**—Select this option to ensure that a given certificate chain (from the supplied certificate to the root Certificate Authority's certificate) is valid and trustworthy.
   - **Certificate Revocation check by CRL**—Select this option to check whether a certificate is revoked (becomes invalid) by looking up the Certificate Revocation List (CRL).
4. Click **Save**.

Client Certificate Handling

For many high-security applications, such as online banking, the Web server may require client certificates to authenticate the clients. Since IWSVA does not support Web sites that require client certificates, you can select to tunnel or block the connection in the Client Certificate Handling screen.

- **Tunnel**—Select this option to bypass HTTPS traffic. IWSVA will not decrypt the content for inspection.
- **Block**—Select this option to deny access to the remote server.

Certificate Authority

By default, IWSVA acts as a private Certificate Authority (CA) and dynamically generates digital certificates that are sent to client browsers to complete a secure session for HTTPS connections. However, the default CA is not signed by a trusted CA on the Internet and the client browsers will display a certificate warning each time users access an HTTPS Web site. Although users can safely ignore the certificate warning, Trend Micro recommends using a signed certificate for IWSVA.

Note: IWSVA supports certificates using base64-encoded format only.
To stop a certificate warning screen from being displayed on user computers when accessing a secured Web site, set the certificate as a trusted certificate for all users.

To import a CA certificate:

1. From the main menu, click **HTTP > HTTPS Decryption > Settings | Certificate Authority**.
2. Click **Browse** next to **Certificate** to select a certificate file. IWSVA supports certificates using base64-encoded format.
3. Click **Browse** next to **Private Key** to select the private key associated with the CA certificate. The private key is provided together with your certificate from the well-known CA.
4. Type the **Passphrase** if you provided this information when you first applied for the certificate.
5. Type the passphrase again the **Confirm Passphrase** field.
6. Click **Import**.

To export a CA certificate (public key):

1. From the main menu, click **HTTP > HTTPS Decryption > Settings | Certificate Authority**.
2. Click **Get Public CA Key**.
3. Follow the on-screen prompt to save the certificate file on your computer.

To export CA private key:

1. From the main menu, click **HTTP > HTTPS Decryption > Settings | Certificate Authority**.
2. Click **Get Private CA Key**.
3. Follow the on-screen prompt to save the key file on your computer.

Creating and Modifying HTTP Virus Scanning Policies

In addition to the default global and guest policies, you can create customized HTTP scanning policies for specified members of your organization.

To create a new virus scan policy:

1. Choose **HTTP > HTTP Scan > Policies** from the main menu.
2. Select **Enable virus scanning** to enable virus scanning.
3. Select **Enable Web Reputation** to enable Web Reputation.

Note: Web Reputation must be enabled at the global level to be used at the policy level.

4. Click **Add**.
5. Type a descriptive **Policy name**.

   Policy names that include references to the users or groups to which they apply (for example, "Virus Policy for Engineers" or "URL Filtering Policy for Researchers") are easy to remember.
6. Select the users to which this policy applies.

   The options on this page depend upon the user identification method that you are using—either **IP address**, **Host name (modified HTTP headers)**, or **User/group name authentication**. For more information about configuring the user identification method and defining the scope of a policy, see Configuring the User Identification Method starting on page 6-5 and LDAP Query Matching Across Main and Referral Servers starting on page 6-21.

Note: Regardless of the user identification method you have configured, you can always enter IP addresses of the clients to which the policy applies.

7. When you have named your new policy and defined the account(s) to which it applies, click **Next** to proceed with defining HTTP virus scanning rules.

To modify an existing HTTP scanning policy:

1. Click **HTTP > HTTP Scan > Policies** from the main menu.
2. Click the name of the policy to modify.
3. Modify the Web Reputation rule, virus scanning rule, the spyware scanning rule, policy exceptions, and the scanning action.

   The specified scanning action applies to all specified rules.

To add or remove users from an existing HTTP scanning policy:

1. Click **HTTP > HTTP Scan > Policies** from the main menu.
2. Click the desired scan policy account.
3. From the **Scan Policy: Edit Policy** screen, on the **Account** tab, either add or remove a user.
   - To add a user, specify a user IP address in the **IP address** field or specify a range of users in the **From** and **To** fields under **IP range.** Click **Add** after specifying a user or range of users.
   - To remove a user, click the trash can icon next to the user.

To enable a HTTP scanning policy:

- In any HTTP scanning policy configuration page, select **Enable policy**.

Specifying Web Reputation Rules

Web Reputation rules are created at the policy level.

To specify Web Reputation rules:

1. Ensure that Web Reputation is enabled at the global level.

   Web Reputation must be enabled at the global level to use it at the policy level (**HTTP > HTTP Scan > Policies | Enable Web Reputation** checkbox).
2. Ensure that Web Reputation is enabled at the policy level.

Using the **Add** or **Edit** option for the **HTTP > HTTP Scan > Policies | Web Reputation Rule** page, ensure that the **Use Web Reputation rule in this policy** check box is selected. This check box is selected by default.

3. Select **Use Page Analysis in this policy** to enable IWSVA to examine the Web site for malicious content and adjust the reputation score. For example, if malicious content is detected on a Web site, IWSVA will decrease its reputation score and block access if the score is below the configured sensitivity threshold.
4. Specify the URL blocking sensitivity level.

   Upon receiving the Web Reputation score, IWSVA determines whether the score is above or below the threshold. The threshold is defined by sensitivity level as configured by the user. Medium is the default sensitivity setting. This setting is recommended because it blocks most Web threats while not creating many false positives.
5. Either accept or disable the anti-pharming and anti-phishing detections.

   By default, anti-pharming and anti-phishing detections are enabled. See Anti-phishing and Anti-pharming Detection on page 7-14.

Anti-phishing and Anti-pharming Detection

Phishing attacks are emails designed to steal private information from you. These emails contain URLs which direct you to imposter Web sites where you are prompted to update private information, such as passwords and credit card numbers, social security number, and bank account numbers.

Pharming attacks are attempts to redirect you to imposter Web sites with the intention of stealing private information, which is usually financially related. Pharming compromises a DNS server by planting false information into the server, which causes a user's request to be redirected to an unintended location. Unfortunately, the Web browser displays what appears to be the correct Web site.

Note: Because the source of anti-phishing/pharming detection is Web Reputation and anti-phishing/pharming functions in an anti-threat capacity, it is therefore part of the Web Reputation Rule for a policy. And because Web Reputation at the policy level cannot function until enabled at the global level, anti-phishing/pharming is also disabled when Web Reputation is disabled globally.

In ICAP mode, IWSVA does not support anti-pharming.

Web Reputation Settings

Web Reputation settings involve specifying the following:

- Whether to provide feedback on infected URLs to Trend Micro
- Whether to evaluate Web Reputation in a monitoring only mode (no URLs are blocked)

Enabling and Disabling Web Reputation

IWSVA allows you to enable or disable Web Reputation at the global level and at the policy level. If you disable Web Reputation at the global level, then it is automatically disabled at the policy level.

To enable and disable Web Reputation at the global level:

1. Click **HTTP > HTTP Scan > Policies** from the main menu.
2. From the Scan Policies screen, select **Enable Web Reputation** to enable Web Reputation. Clear the checkbox to disable it.

To enable and disable Web Reputation at the policy level:

1. Click **HTTP > HTTP Scan > Policies > policy name** and click the **Web Reputation Rule** tab.
2. Select **Use Web Reputation rule in this policy** to enable Web Reputation or clear the check box to disable it for this policy.

Managing Web Reputation Results

IWSVA provides two options for managing Web Reputation results: (1) Provide feedback on infected URLs to help improve the Web Reputation database and (2) monitor the effectiveness of Web Reputation without affecting existing Web-access policies. One or all options can be selected.

Feedback Option

In addition to the current dynamic URL Blocking List, virus scan results can be fed back to the URL Local Cache and an external backend Rating Server. The Trend Micro Feedback Engine (TMFBE) provides a feedback mechanism for IWSVA to send back virus scan results to the backend Rating Server. The Feedback option is enabled by default.

Note: When using Upstream Proxy mode, you might need to configure the proxy server to explicitly allow the IWSVA IP address to access www.trendmicro.com.

Negative Results

If the scan result from the Trend Micro virus scanning engine is negative, the infected URL is sent back to the following locations:

- Dynamic URL Blocking List
- URL Local Cache with an adjusted Web Reputation score
- TMFBE feedback buffer with VirusName and IntelliTrap Flag. When this buffer reaches ten entries or five minutes have passed from the last feedback, these URLs are sent to the backend Rating Server in a batch (each URL is sent sequentially).

Positive Results

If the scan result from Trend Micro's virus scanning engine is positive, the URL in question is saved in the URL local cache. This prevents the same URL from getting scanned by Trend Micro's virus scanning engine twice.

Monitor Only Option

The Monitor Only option gives you the opportunity to evaluate Web Reputation results. With this option selected, you are able to monitor Web Reputation results from the URL Blocking Log or Security Risk Report. The results only include the URLs filtered by Web Reputation, anti-phishing and anti-pharming. Because you are only monitoring Web Reputation results, no URL blocking occurs and URLs are passed to clients.

By default, the Monitor Only option is disabled.

Clearing the WRS/URL Cache

When a user attempts to access a URL, IWSVA retrieves information about this URL from a remote database—the Web Reputation database—and stores the retrieved information in a local WRS/URL cache. Having the Web Reputation database on a remote server and building the local WRS/URL cache with this database information reduces the overhead on IWSVA and improves performance.

The following are the information types the WRS/URL cache can receive from the Web Reputation database for a requested URL:

- Web category
- Pharming and phishing flags used by anti-pharming and anti-phishing detection
- Web Reputation rating results used to determine whether or not to block a URL (see Specifying Web Reputation Rules on page 7-13)

The URL cache keeps frequently accessed URLs in cache for quick retrieval. Clear the cache only if a new URL query is necessary or if the cache size is affecting performance.

Note: Clearing the cache stops and restarts the HTTP scanning daemon, which may interrupt IWSVA service.

To clear the WRS/URL cache:

1. From the main menu, click **HTTP > Configuration > WRS/URL Cache**.
2. Click **Clear Cache**.

Using the Content Cache

Web content caching is the caching of Web objects (such as HTML pages and images) to reduce bandwidth usage, server load, and perceived lag. A Web cache stores copies of objects passing through it. Subsequent duplicate requests may be satisfied from the cache if certain conditions are met. Cached objects will be re-scanned by IWSVA.

The Content Cache capability provides users who access the Web through IWSVA with a quicker experience while saving bandwidth.

Note: This feature is available only in Forward Proxy mode. If the deployment mode changes from Forward Proxy mode to another mode, the Content Cache feature is grayed out and will not function.

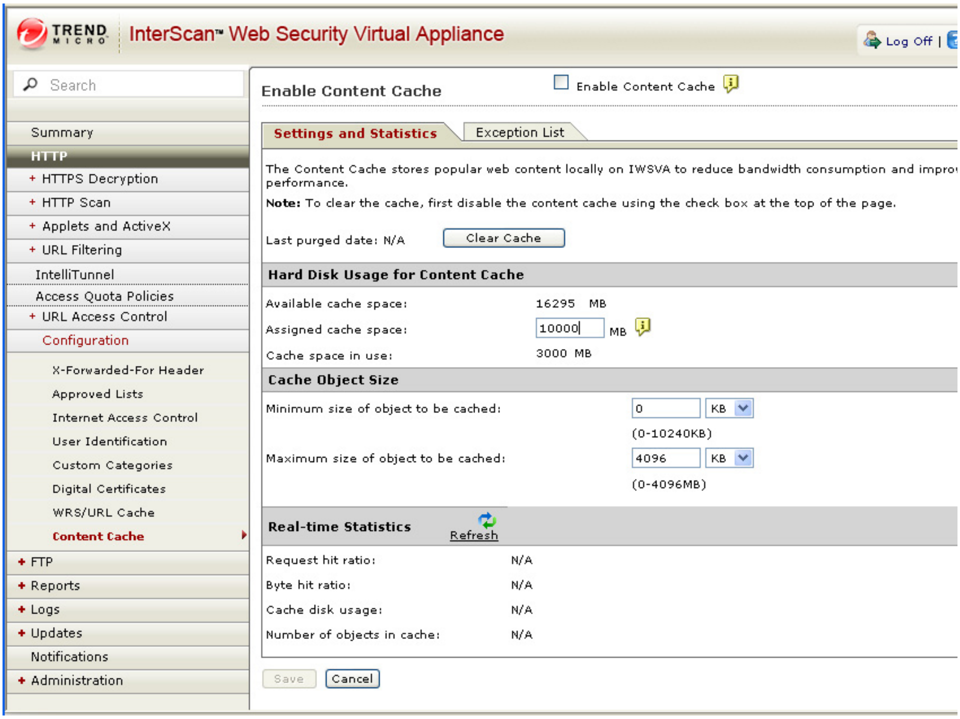
With the Content Cache feature, administrators enable or disable the IWSVA in-box cache and manage caching through Web console. It also generates cache statistics.

Note: The Content Cache feature cannot be disabled from the CLI.

Enabling/Disabling the Content Cache

To enable/disable the Content Cache feature:

1. Go to **HTTP > Configuration > Content Cache**.
2. Select the **Enable Content Cache** check box at the top of the page to enable the Content Cache feature. (See *Figure 7-3*.)
3. Click **Save**.
4. Clear the **Enable Content Cache** check box to disable the Content Cache feature.
5. Click **Save**.



Enable Content Cache

□ Enable Content Cache

The Content Cache stores popular web content locally on IWSVA to reduce bandwidth consumption and impro performance.

Note: To clear the cache, first disable the content cache using the check box at the top of the page.

Last purged date: N/A

Hard Disk Usage for Content Cache

Available cache space:	16295 MB
Assigned cache space:	10000 MB
Cache space in use:	3000 MB

Cache Object Size

Minimum size of object to be cached:	0 KB (0-10240KB)
Maximum size of object to be cached:	4096 KB (0-4096MB)

Real-time Statistics

Request hit ratio:	N/A
Byte hit ratio:	N/A
Cache disk usage:	N/A
Number of objects in cache:	N/A

FIGURE 7-3. Content Cache screen

Clearing the Content Cache

To clear the Content Cache:

1. Disable the Content Cache feature before clearing the cache.

   The Clear Cache button is disabled when the Content Cache feature is enabled.

2. Click **Clear Cache**. You receive the following warning:

   “It could take a significant amount of time to clear a large cache.

   Are you sure you want to clear the cache?”

3. Click **OK**. A progress bar displays during the cache clearing process.

The Clear Cache button and the Enable Content Cache checkbox are both disabled until the clearing process ends. After the cache clears, the "Last purged date" updates.

Managing the Content Cache

Administrators can configure the following content cache areas:

- Hard disk usage for the Content Cache
- Cache object size

To manage the Content Cache:

1. Go to the **Hard Disk Usage for Content Cache** section of the Content Cache Settings and Statistics tab.
2. Enter a quantity for the **Cache space size**. (See *Figure 7-3*.)

   Administrators can adjust the amount of disk space used to store the cached content. A larger cache volume will allow more Web objects to be cached. A smaller cache partition will reduce the number of cacheable objects. If you set the cache volume too small and run out of disk space for caching, the hit ratio may decrease as IWSVA will rely more on real-time content retrieval and less on locally cached content.

   Perhaps your VA total partition space is 40GB within binaries, files and log occupying 15GB. Currently, your "Assigned cache space" setting may be 10GB, and the "Cache space in use" may be 5GB. The screen show:

   - Available cache space: 25,000MB [40GB (total space) - 15GB (logs, miscellaneous)]
   - Assigned cache space: 10,000MB
   - Cache space in use: 5,000MB

   In this case, the "Assigned cache space" setting could be increased to a maximum of 25GB.
3. To tune the minimum and maximum size values, select the amount and unit of measure (KB/MB) for the following:
   - Minimum size of object to be cached (default 0KB) Range allowed is: 0-10240KB/10MB
   - Maximum size of object to be cached (default 10MB) Range allowed is: 1-4096MB/4194304KB

The minimum size and maximum size of cached objects will allow you to tune the caching performance. If the minimum size of cached objects is set too small, the cache service will use local resources to cache content that can be retrieved more quickly from the Internet and this can slow performance. If the minimum size is set too large, the cache may not contain popular objects that can save bandwidth and reduce latency.

This is similarly true for the maximum size of cacheable objects. Depending on the type of Web pages users access what type of cacheable objects they contain, the performance will vary. You can experiment with the minimum and maximum size values to fine tune the cache performance and hit rate for your environment. Trend Micro recommends starting with the default values and then fine tuning as necessary for your environment.

4. Click **Save**.

Content Cache Real-time Statistics

The real-time statistics for the Content Cache feature include:

TABLE 7-1. Real-time Statistics definitions

CACHE STATISTICS	DESCRIPTION
Request hit ratio	The percentage of HTTP requests that result in a cache hit.
Byte hit ratio	Compares the number of bytes received from origin servers to the number of bytes sent to clients. When received bytes are less than sent bytes, the byte hit ratio is positive. However, a negative byte hit ratio may occur if clients abort multiple requests before receiving the entire response.
Cache disk usage	The amount of data currently cached on disk.
Number of objects in cache	Represents the number of objects cached.

Note: Real-time statistics for the Content Cache feature will not refresh automatically. You must click the Refresh link for the statistics to update.

Content Cache Exceptions List

When administrators do not want to cache a specific URL, they can add the URL to the cache exceptions list. The behavior here is the same as the URL blocking list. Administrators can add a Web site, URL keyword, or string to exceptions list. URLs that match the list will not be cached by IWSVA.

You can have IWSVA block certain Web pages, domains, and URLs from being stored in the content cache. URLs blocked from the Content Cache are not policy based—it affects everyone in the organization.

Note: Content caching is only supported in Forward Proxy mode.

Blocking URLs from the Content Cache combats large Web sites from being cached and taking up cache space that is more efficiently used for other common Web sites.

- **Enable Content Cache**—Enable or disable Content Cache (click Save after enabling or disabling content caching).
- **Match**—Enter an exact Web site, a keyword or phrase, or a string of characters in the field, and then configure IWSVA with how to apply the match. URLs blocked from the content cache supports both the ? and * wildcard.
- **Web site**—Limits the search to the string as a whole; used with one or more wildcards, this type of blocking can be especially useful for preventing entire Web sites from being cached. There is no need to include http:// or https:// in the URL (as it is automatically stripped).
- **URL Keyword**—Looks for any occurrence of the letters or numbers within a URL, and will match regardless of where the string is found (the string "sex" would be considered a match for "http://www.encyclopedia/content/sexton.htm" and the page blocked. Using wildcards with URL Keywords greatly increase the chance of false positives.
- **String**—Limits the search to the string as a whole; for example, to target a specific site, page, file, or other particular item.

- **Import Blocked Content Cache List and Exception**s—You can import an existing list of URLs that you want to block or exempt from content caching. For example, if you have a list of URLs from a third-party vendor, Web Manager, or related software program, or a list of sites you have compiled using a text editor, you can import the list rather than enter them one-by-one in the Match field. Imported lists must conform to a defined standard.

Content Cache Exceptions List Format

The Content Cache exception list uses the following format to import exception lists.

```
[no_cache]

www.example.com/subdomain*

*example.com*

www.example.com/c.jgp

www.example.com*

*www.example1.com*

www.example2.com
```

HTTP Virus Scanning Rules

IWSVA administrators can configure which file types to block and scan, and how compressed and large files are handled.

Specifying File Types to Block

You can identify the types of files to block for security, monitoring, or performance purposes. Blocked files are not received by the requesting client or scanned—requests to retrieve a blocked file type are not executed. You have the option of blocking file types such as Java applets, executables, Microsoft Office documents, audio/video files, images or other files types that you specify.

To specify which file types to block:

1. While adding or editing a policy, under **Block These File Types**, check the box of the file types to block. This will block all files in that category.
2. To choose to unblock file types within a selected category, click the Show Details link.
3. Uncheck the files that should not be blocked.

Specifying File Types to Scan

IWSVA is equipped with the following HTTP scanning capabilities:

- IntelliScan
- True-file type detection
- IntelliTrap

Note: For the highest level of security, Trend Micro recommends scanning *all* files.

About IntelliScan

Most antivirus solutions today offer you two options to determine which files to scan for potential risks. Either all files are scanned (the safest approach), or only those files with certain file extensions considered the most vulnerable to infection are scanned. However, recent developments that disguise files by changing their extensions renders this latter option less effective. *IntelliScan* is a Trend Micro technology that identifies a file's "true-file type," regardless of the file name extension.

Note: IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible to virus infection.

About True-file Type

When set to scan *true*-file type, the scan engine examines the file header rather than the file name to ascertain the actual file type. For example, if the scan engine is set to scan all executable files and it encounters a file named `family.gif`, it will not accept that the file is a graphic file and skip scanning. Instead, the scan engine opens the file header and examines the internally registered data type to determine whether the file is indeed a graphic file, or, for example, an executable that has been deceptively named to avoid detection.

True-file type scanning works in conjunction with Trend Micro IntelliScan, to scan only those file types known to be of potential danger. These technologies can mean a reduction in the overall number of files that the scan engine must examine (perhaps as much as a two-thirds reduction), but it comes at the cost of potentially higher risk.

For example, .GIF and .JPG files make up a large volume of all Web traffic. It is possible for a malicious hacker to give a harmful file a “safe” file name to smuggle it past the scan engine and onto the network. The file could not run until it was renamed, but IntelliScan would not stop the code from entering the network.

To select which file types to scan:

IWSVA can scan all files that pass through it, or just a subset of those files as determined by true-file type checking (IntelliScan) or the file extension. In addition, individual files contained within a compressed file can also be scanned.

1. Select the files to scan:
   - To scan all file types, regardless of file name extension, select **All scannable files**. IWSVA opens compressed files and scans all files within. This is the most secure, and recommended, configuration.
   - To use true-file type identification, select **IntelliScan**. This configuration scans file types that are known to harbor viruses by checking the file’s true-file type. Because checking the true-file type is independent of the filename’s extension, it prevents a potentially harmful file from having its extension changed to obscure its true-file type.
   - You can explicitly configure the types of files to scan or skip, based on their extensions, to work around possible performance issues with scanning all HTTP traffic. However, this configuration is not recommended because the file extension is not a reliable means of determining its content.

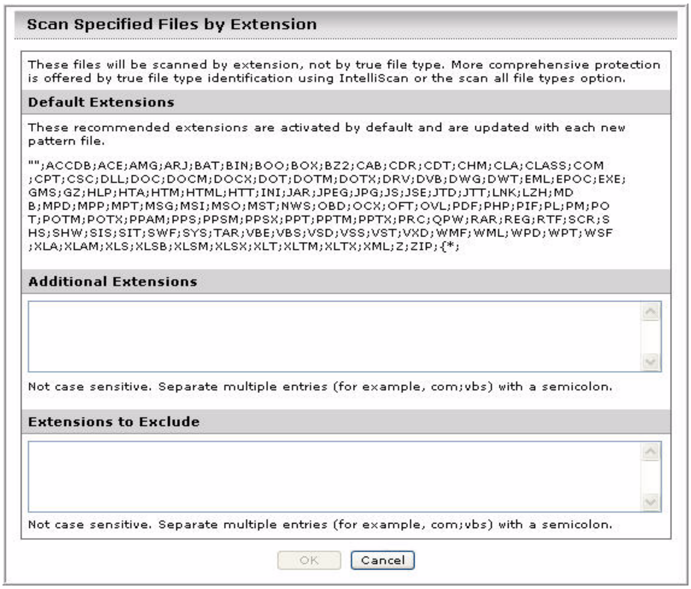
To scan only selected file types, select **Specified file extensions** and then click the list. (Trend Micro does not recommend this setting.) The **Scan Specified Files by Extension** screen opens. The default extensions list shows all file types that are known to potentially harbor viruses. This list is updated with each virus pattern file release. On the **Scan Specified Files by Extension** screen, add or exclude additional extensions in the **Additional Extensions** and **Extensions to Include** fields.

Enter the extension to scan or exclude from scanning (typically three characters), without the period character. Do not precede an extension with a wildcard (*) character, and separate multiple entries with a semicolon.

Click **OK** when you are finished. The screen closes.

2. You can configure IWSVA to selectively bypass certain MIME content-types. Some file types, such as RealAudio or other streaming content, begin playing as soon as the first part of the file reaches the client machine and does not work properly with the resulting delay. You can have IWSVA omit these file types from scanning by adding the appropriate MIME types to the **MIME content-types to skip** list on the **Virus Scan Rule** tab. Type the MIME content-type to bypass in the **MIME content-type to skip** field (for example, image, audio, application/x-director video, and application/pdf). See Appendix B, *Mapping File Types to MIME Content-types* for more information.

Note: Trend Micro recommends minimizing the list of MIME content-types to skip to reduce the risk of virus infection. Also, Trend Micro does not recommend skipping any MIME content-types when large file handling is enabled, because it's possible for a MIME content-type to be forged.



Scan Specified Files by Extension

These files will be scanned by extension, not by true file type. More comprehensive protection is offered by true file type identification using IntelliScan or the scan all file types option.

Default Extensions

These recommended extensions are activated by default and are updated with each new pattern file.

"";ACCDB;ACE;AMG;ARJ;BAT;BIN;BOO;BOX;BZ2;CAB;CDR;CDT;CHM;CLA;CLASS;COM
;CPT;CSC;DLL;DOC;DOCM;DOCX;DOT;DOTM;DOTX;DRV;DVB;DWG;DWT;EML;EPOC;EXE;
GMS;GZ;HLP;HTA;HTM;HTML;HTT;INI;JAR;JPEG;JPG;JS;JSE;JTD;JTT;LNK;LZH;MD
B;MPD;MPP;MPT;MSG;MSI;MSO;MST;NWS;OBD;OCX;OFT;OVL;PDF;PHP;PIF;PL;PM;PO
T;POTM;POTX;PPAM;PPS;PPSM;PPSX;PPT;PPTM;PPTX;PRC;QPW;RAR;REG;RTF;SCR;S
HS;SHW;SIS;SIT;SWF;SYS;TAR;VBE;VBS;VSD;VSS;VST;VXD;WMF;WML;WPD;WPT;WSF
;XLA;XLAM;XLS;XLSB;XLSM;XLSX;XLT;XLTM;XLTX;XML;Z;ZIP;{*;

Additional Extensions

Not case sensitive. Separate multiple entries (for example, com;vbs) with a semicolon.

Extensions to Exclude

Not case sensitive. Separate multiple entries (for example, com;vbs) with a semicolon.

FIGURE 7-4. The Recommended Extensions to Scan are Updated with Each New Pattern File

About IntelliTrap

IntelliTrap detects potentially malicious code in real-time, compressed executable files that arrive with HTTP data. Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of compressed files that helps reduce the risk that a virus compressed using these methods enters a network through the Web.

IntelliTrap has the following options:

- Can be enabled or disabled in the **Virus Scan Rule** tab for each scan policy. (IntelliTrap is enabled by default.)
- Malicious, compressed executable files receive the actions specified in the Action tab.

To enable / disable IntelliTrap:

- Click **HTTP > HTTP Scan > Policies | <policy name>| Virus Scan Rule tab** and select the **Enable IntelliTrap** check box in the IntelliTrap section.

For more IntelliTrap information, see IntelliTrap Pattern and IntelliTrap Exception Pattern Files on page 4-8.

Priority for HTTP Scan Configuration

IWSVA scans according to the following priority:

1. MIME content-types to skip
2. File types to block
3. File types to scan

Configuring Compressed File Scanning Limits

Compressed file scanning limits can be configured for each policy (click **HTTP > HTTP Scan > Policies > policy** and click the **Virus Scan Rule** tab). IWSVA opens and examines the contents of compressed files according to the criteria specified in the HTTP virus scanning configuration screen. IWSVA decompresses the files according to the configurable limits (number of files in the compressed archive, size of the compressed file, number of compressed layers, and the compression ratio).

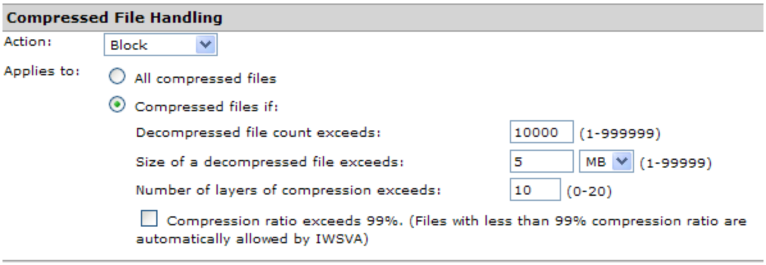
To configure the compressed file scanning limits:

Under **Compressed File Handling**, configure the following settings:

- **Action**: Select an action (**Pass**, **Block**, or **Quarantine**) you want IWSVA to take when it detects a compressed file violation.
- **Applies to**: Select one of the following options.
  - **All compressed files**: Match all requests to download compressed files.
  - **Compressed files if...**: Match only requests to download compressed files that exceed the configured criteria. Type values for the following parameters:

- Decompressed file count exceeds (default is 50000)
- Size of a decompressed file exceeds (default is 200MB)
- Number of layers of compression exceeds (range is 0-20; default is 10)
- Enable/disable Compress ratio exceeds 99% (default is disable)

IWSVA applies the selected action on a compressed file that meets the specified conditions at the gateway and the file is not scanned. For example, suppose your settings appear as shown in *Figure 7-5*:



Compressed File Handling

Action: Block

Applies to:

○ All compressed files

● Compressed files if:

Decompressed file count exceeds: 10000 (1-999999)

Size of a decompressed file exceeds: 5 MB (1-99999)

Number of layers of compression exceeds: 10 (0-20)

□ Compression ratio exceeds 99%. (Files with less than 99% compression ratio are automatically allowed by IWSVA)

FIGURE 7-5. "Decompression percent" can be used to prevent a denial-of-service (DoS) attack against the IWSVA device

A compressed file that has more than 10 layers of compression or contains more than 10000 files that will not pass through the gateway.

Handling Large Files

For larger files, a trade-off must be made between the user's experience and expectations, and maintaining security. The nature of virus scanning requires doubling the download time (that is, the time transferring the entire file to IWSVA, scanning the file, and then transferring the entire file to the client) for large files. In some environments, the doubling of download time might not be acceptable. There are other factors such as network speed, and server capability that must be considered. If the file is not big enough to trigger large-file handling, the file is scanned as a normal file.

Consider configuring large file handling if your users experience browser time-outs when trying to download files. There are two large file scanning options:

- Scan Before Delivering (Progress Page) on page 7-30
- Deferred Scanning on page 7-31

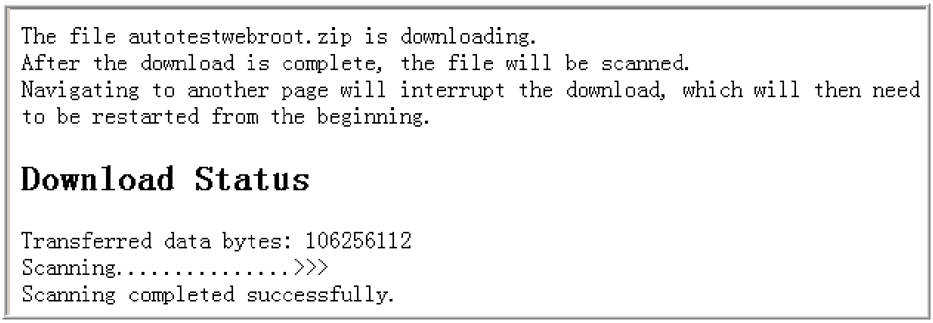
Scan Before Delivering (Progress Page)

When IWSVA is configured to use the **Scan before delivering** scanning option, requested files are not passed to the client until scanning is finished. A progress page is generated to prevent the browser from timing out and to inform the user that scanning is in progress to prevent them from thinking that the connection is hung.

Note: For large file handling, IWSVA uses the progress page. The progress page uses JavaScript and a pop-up window to display the download progress. If your desktop security policy has pop-up blocking enabled or JavaScript disabled, then the progress page does not function and scanning is prevented.

For the progress page to work, IWSVA needs to determine to which externally visible IP address the clients connect. Using 127.0.0.1 causes a problem. If a message about the progress page appears, add the machine IP address to `iscan_web_server` so that the host name does not resolve to 127.0.0.1 (for example, `iscan_web_server=1.2.3.4:1812`) or modify the `/etc/hosts` file

.



The file autotestwebroot.zip is downloading.
After the download is complete, the file will be scanned.
Navigating to another page will interrupt the download, which will then need to be restarted from the beginning.

Download Status

Transferred data bytes: 106256112
Scanning..............>>>
Scanning completed successfully.

FIGURE 7-6. "Scan before delivering" Large File Handling Progress Window

Note: Some Internet applications (YouTube, Windows Update, streaming, and others) are programmed to receive a certain amount of data on the client side within a certain time frame (for example, 20 percent of data or 1MB of data in 90 seconds). When IWSVA is configured to use the Scan feature before delivering the scanning option, some requested files will not be passed to the client until the scanning is completed. In this case, it is likely that the Internet application could detect a transmission failure because the client side does not receive enough data in time. Then, the client side will not be able to complete the video file or streaming file.

Deferred Scanning

When IWSVA is configured to use the **Deferred scanning** option, part of the file is passed to the requesting client while IWSVA scans the remainder of the file. The partial file remains in the client's temporary directory until scanning concludes and the last byte of the file is delivered.

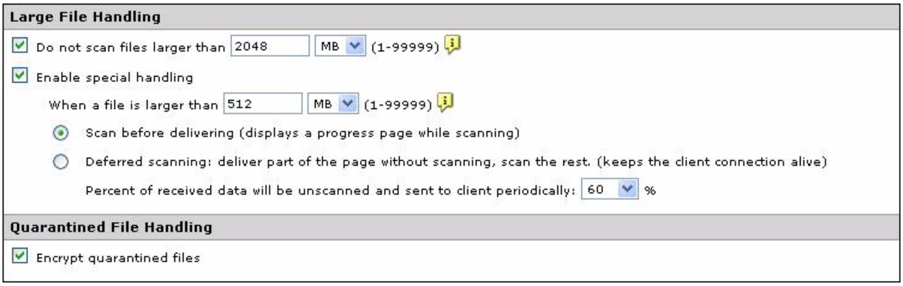
Instead of using a specified data size, IWSVA uses a percentage to define how much data is downloaded at a time. At most every two seconds, IWSVA sends a specified percentage of received data to the browser. The last chunk of data is not larger than 4KB and is sent to the browser before the scan is finished.

For the data download percentage, you can specify either 20, 40, 60, 80, or 100. The default percentage is 60. The actual percentage of data sent to the browser can be much smaller than the percentage specified.

Note: Large file handling does not work when using the Blue Coat Port 80 Security Appliance in ICAP mode. In addition, when using the Blue Coat security appliance in ICAP mode, when the client downloads a large virus-infected file, the client browser may not show the virus blocking notification page. Instead, the client browser will show "Page cannot be displayed." If IWSVA is configured as an HTTP proxy in-line with the Blue Coat appliance, however, large file handling functions.

External data received by IWSVA is sent to the browser in smaller chunks without scanning. The last chunk is sent to the browser to complete the download only after the entire set of data is received and scanned. Sending smaller chunks not only maintains the IWSVA-Web browser connection, but also keeps end-users posted of the download progress.

Large file handling can be set for each policy (click **HTTP > HTTP Scan > Policies > policy** and click the **Virus Scan Rule** tab).



Large File Handling

☑ Do not scan files larger than 2048 MB (1-99999)

☑ Enable special handling

When a file is larger than 512 MB (1-99999)

● Scan before delivering (displays a progress page while scanning)

○ Deferred scanning: deliver part of the page without scanning, scan the rest. (keeps the client connection alive)

Percent of received data will be unscanned and sent to client periodically: 60 %

Quarantined File Handling

☑ Encrypt quarantined files

FIGURE 7-7. For special handling of large files, there are two options to choose from: (1) scan before delivering and (2) deferred scanning

Disable large file scanning by choosing the **Do not scan files larger than** option to reduce performance issues when downloading very large files. This allows you control over their integrity.

To disable scanning large files:

- Under **Large File Handling**, select the **Do not scan files larger than** check box and then configure the file size over which files are not scanned. The default is 2048MB.

  Trend Micro does not recommend disabling the scanning of any files, even large ones, because it introduces a security vulnerability into your network.

To use large file handling for HTTP scanning:

1. In the **Large File Handling** section, select **Enable special handling**, and then type the file size (in KB or MB) to be considered a large file.

   The default value is 512KB.

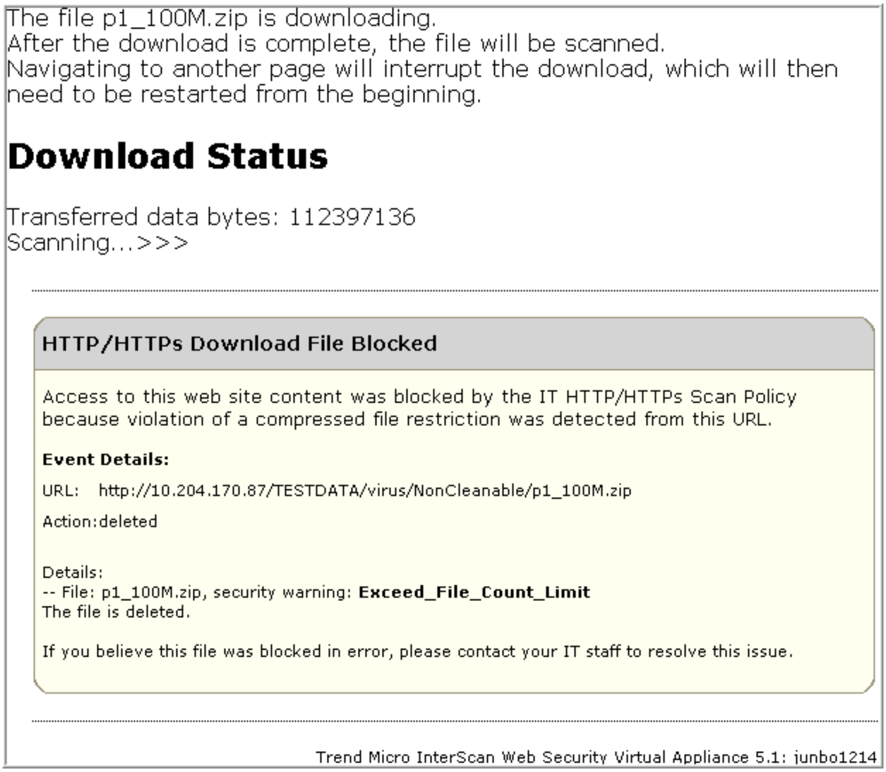
2. Select the type of large file-handling to use:

   - **Scan before delivering**: Shows progress while scanning, and then loads the page afterwards (default setting)
   - **Deferred scanning**: Loads part of the page while scanning; stops the connection if a virus is found

3. Click **Save**.

Important Notes for Large File Handling

- Violations of the large file handling policy displays a user notification in the requesting client's browser. See the example in *Figure 7-8*.



The file p1_100M.zip is downloading.
After the download is complete, the file will be scanned.
Navigating to another page will interrupt the download, which will then need to be restarted from the beginning.

Download Status

Transferred data bytes: 112397136
Scanning...>>>

HTTP/HTTPs Download File Blocked

Access to this web site content was blocked by the IT HTTP/HTTPs Scan Policy because violation of a compressed file restriction was detected from this URL.

Event Details:

URL: http://10.204.170.87/TESTDATA/virus/NonCleanable/p1_100M.zip

Action:deleted

Details:
-- File: p1_100M.zip, security warning: **Exceed_File_Count_Limit**
The file is deleted.

If you believe this file was blocked in error, please contact your IT staff to resolve this issue.

Trend Micro InterScan Web Security Virtual Appliance 5.1: junbo1214

FIGURE 7-8. Notification after Completing Scanning and Downloading the File

- Large file special handling only applies to HTTP scanning, FTP scanning, and FTP over HTTP through the HTTP proxy. It does not apply to FTP over HTTP for ICAP traffic. Time-out issues may occur while downloading large files using FTP over HTTP.
- When using the deferred scanning method, IWSVA does not delete files subsequently found to be infected in the first affected client.

Quarantined File Handling

If you choose to quarantine files that IWSVA detects as malicious, you can optionally choose to encrypt the files before moving them to the quarantine folder by selecting the **Encrypt quarantined files** check box.This prevents the files from being inadvertently executed or opened. Note that encrypted files can only be decrypted by a Trend Micro Support engineer.

After configuring the HTTP virus scanning rules in the **HTTP > HTTP Scan > Policies > Add Policy /Edit Policy** screen, click **Next** to move on to the spyware/grayware scanning rules.

Spyware and Grayware Scanning Rules

In addition to computer viruses, the IWSVA pattern files include signatures for many other potential risks. These additional risks are not viruses, because they do not replicate and spread. However, they can perform unwanted or unexpected actions, such as collecting and transmitting personal information without the user's explicit knowledge, displaying pop-up windows, or changing the browser's home page.

IWSVA can be configured to scan for the following additional risks:

- **Spyware—**Software that secretly collects and transmits information without the user's explicit knowledge or consent
- **Dialers—**Software that secretly dials a telephone number, typically an international or pay-per call number, through the user's modem.
- **Hacking tools—**Software that can be used for malicious hacking purposes.
- **Password cracking programs—**Software designed to defeat computer passwords and other authentication schemes.

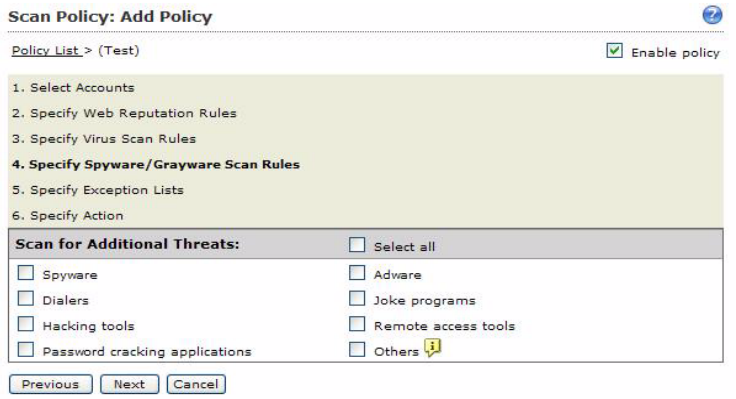
- **Adware—**Software that monitors and collects information about a user's browsing activities to display targeted advertisements in the user's browser or through pop-up windows.
- **Joke programs—**Programs that mock computer users or generate some other sort of humorous display.
- **Remote access tools—**Programs designed to allow access to a computer, often without the user's consent.
- **Others—**Files that do not fit into the other additional risks classifications. Some of these might be tools or commercial software that have legitimate purposes, in addition to having the potential for malicious actions.

To scan for spyware, grayware, and other non-virus additional risks:

1. Click **HTTP > HTTP Scan > Policies > policy** and click the **Spyware/Grayware Rule** tab. Under **Scan for Additional Threats**, select the types of additional risks to be detected.

   To scan for all additional risks that have signatures in the pattern file, check **Select All**.

2. Click **Next** to configure the actions against security risks.



Scan Policy: Add Policy

Policy List > (Test) ☑ Enable policy

1. Select Accounts
2. Specify Web Reputation Rules
3. Specify Virus Scan Rules
4. **Specify Spyware/Grayware Scan Rules**
5. Specify Exception Lists
6. Specify Action

Scan for Additional Threats: □ Select all

□ Spyware	□ Adware
□ Dialers	□ Joke programs
□ Hacking tools	□ Remote access tools
□ Password cracking applications	□ Others

FIGURE 7-9. Spyware, grayware and additional threat scan configuration

X-Forwarded-For HTTP Headers

The X-Forwarded-For (XFF) HTTP header is a de facto standard for identifying the originating IP address of a client connecting to a Web server through an HTTP proxy or load balancer. X-Forwarded-For header is supported by most proxy servers.

- When IWSVA receives an HTTP request with XFF header, it parses the XFF header to get the original client IP address and use the IP address to do policy match.
- When IWSVA forwards an HTTP request, it takes the action configured by the administrator on XFF HTTP header. (See *Table 7-1*.)

Note: IWSVA does not support parsing XFF headers for HTTPS traffic.

TABLE 7-1. Available actions for XFF HTTP headers

ACTION	DESCRIPTION
Keep	(Default) IWSVA does not make any changes to the XFF HTTP header.
Append	IWSVA adds the IP address of last hop into the XFF HTTP header. If the XFF HTTP header does not exist, IWSVA creates one.
Strip	IWSVA removes the XFF HTTP header from the HTTP request and prevents the privacy information of client from leaking upstream.

See *Table 7-2* to verify that your deployment scenario works with the XFF HTTP headers.

TABLE 7-2. Deployment scenarios using X-Forwarded For HTTP headers

DEPLOYMENT MODE	PARSES XFF	ACTION: KEEP	ACTION: ADD IP ADDRESS	ACTION: REMOVE	NOTES
Forward Proxy	Yes	Yes	Yes	Yes	

TABLE 7-2. Deployment scenarios using X-Forwarded For HTTP headers

DEPLOYMENT MODE	PARSES XFF	ACTION: KEEP	ACTION: ADD IP ADDRESS	ACTION: REMOVE	NOTES
Bridge	Yes	Yes	N/A	Yes	This mode is transparent and does not need to add and IP address in the header.
WCCP	Yes	Yes	Yes	Yes	
Simple Transparency	Yes	Yes	Yes	Yes	
ICAP	N/A	N/A	N/A	N/A	IWSVA acts as an ICAP server. It does not communicate with the client and server. The IP address is provided by the ICAP client with an X-Client-IP header
Reverse Proxy	N/A	N/A	N/A	N/A	XFF HTTP headers are not supported in this mode.

Configuring X-Forwarded-For HTTP Headers

In IWSVA, there are mainly two scenarios to configure:

- Enabling or disabling the parsing of XFF HTTP headers
- Configuring the action taken on the XFF HTTP header (if enabled.)

To configure the XFF HTTP header module settings:

1. Go the **HTTP > Configuration > X-Forwarded-For Header.**
2. Enable or disable parsing of the XFF HTTP.
    - To enable, select **Enable** from the drop-down list.
    - To disable, select **Disable** from the drop-down list.
3. If parsing is enabled, set the action to **Keep** (default) the X-Forwarded-For header intact, **Append** the IP address where the IWSVA receives the request**,** or **Strip** the X-Forwarded-For header. (See *Table 7-1*.)
4. Click **Save**.

Specifying the Exception Lists

The following describes the type of exception list you can apply to a policy:

- **URL exception list**—contains a list of Web site URLs that you want to exempt from a URL filtering policy, HTTPS decryption policy, Applet/ActiveX security policy, or the WRS rule and file type blocking in an HTTP scanning policy.
- **File name exception list**—files that you want to exempt from file type blocking.

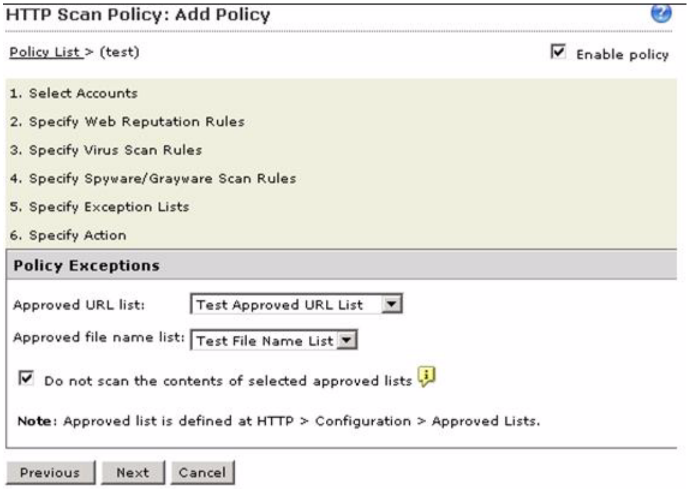
In addition, you can configure IWSVA to bypass virus/spyware scanning and compressed file handling action on an approved list. This could cause security holes when this approved Web site has been hacked to inject malicious code into the Web site. IWSVA addresses this issue by enabling the virus/spyware scan feature as the default. As such, the Web page is always scanned even when a security policy determines that the Web site is within its approved list.

You can apply an exception list in the Policy Exception screen. For HTTP and FTP scanning policies, you can also apply a filename exception list. You can create new exception lists in the Approved Lists screen (see *Creating Exception Lists* on page 7-39 for more information).

The following describes the options in the Policy Exception screen:

- **Approved URL list**—Select the name of the approved URL list to be exempted from a URL filtering policy, HTTPS decryption policy, Applet/ActiveX security policy, or the WRS rule and file type blocking in an HTTP scanning policy.

- **Approved file name list**—Select a file name list to be exempted from file type blocking. You can apply a file name exception list to an HTTP scanning policy or an FTP scanning policy. This option is not available for Applets and ActiveX policies and URL filtering policies.
- **Do not scan the contents of selected approved lists**—Select this option if you do not want to scan the contents of the URLs or files in the approved lists for viruses. Compressed file handling is not available when this option is selected.



HTTP Scan Policy: Add Policy

Policy List > (test)

☑ Enable policy

1. Select Accounts
2. Specify Web Reputation Rules
3. Specify Virus Scan Rules
4. Specify Spyware/Grayware Scan Rules
5. Specify Exception Lists
6. Specify Action

Policy Exceptions

Approved URL list: Test Approved URL List

Approved file name list: Test File Name List

☑ Do not scan the contents of selected approved lists

Note: Approved list is defined at HTTP > Configuration > Approved Lists.

FIGURE 7-10. Configuring policy exceptions

Creating Exception Lists

You can create a new URL and file name exception list in the Approved Lists screen.

To configure a URL exception list:

1. Select **HTTP > Configuration > Approved Lists** from the main menu and click the **URL Lists** tab.
2. Click **Add** and specify a name, the match type or, if preferred, import the URL exception list.
    - **List Name**—Type a brief but descriptive name for the approved list.

- **Match**—Type a Web site, a keyword or phrase, or a string of characters in the field. This field supports both the ? and * wildcards. Entries in this field are added one-by-one to the Approved List.

3. Select the option that corresponds to what you typed in the Match field:
   - **Web site**—Limits the search to the string as a whole; used with one or more wildcards, this type of exemption rule can be especially useful for allowing access to an entire Web site. There is no need to include http:// or https:// in the URL (it is automatically stripped).
   - **URL keyword**—Looks for any occurrence of the letters and/or numbers within a URL, and will match regardless of where the string is found (the string "partner" would be considered a match for "http://www.playboy.com/partner.htm" and the URL exempted). Using wildcards in this field greatly increases the chance of false positives and unexpected results.
   - **String**—Limits the search to the string as a whole; for example to target a specific site, page, file, or other particular item.

Note: - For HTTPS decryption policies, the strings to match vary depending on whether you set IWSVA in the proxy or transparency modes.

- In the proxy mode, IWSVA matches the domain names, not the full URL. Thus, you only need to specify the domain names.

- In the transparency mode (WCCP or bridge mode), IWSVA matches the `CommonName` in the server certificates received.

- For HTTPS standard ports, IWSVA matches the `CommonName`.

- For HTTPS non-standard ports, IWSVA matches `CommonName:Port`

- **Import approved list**—You can import an existing list of URLs that you want exempt from virus scanning or filtering (done by the URL Filtering module). For example if you have a list of URLs from the Trend Micro WebManager, or URLs you have compiled using a text editor, you can import the list rather than enter them one-by-one. Import lists must conform to a defined standard. See *Approved List Formats* on page 7-41.

4. Click **Save**.

To configure a file name exception list:

1. Select **HTTP > Configuration > Approved Lists** from the main menu and click the **File Name Lists** tab.
2. Click **Add** or **Edit** and specify the match type or import the exception list.
   - **List Name**—Type a brief but descriptive name for the approved list.
   - **Match**—Enter a file name with the file extension or a file extension in the field. This field supports the * wildcard. Entries in this field are added one-by-one to the Approved List.
   - **Import approved list**—You can import an existing list of file names that you want exempt from virus scanning. For example if you have a list of file names from Trend Micro's Web site, or file names that you have compiled using a text editor, you can import the list rather than enter them one-by-one. Import lists must conform to a defined standard. See *Approved List Formats* on page 7-41.
3. Click **Save**.

Approved List Formats

IWSVA supports two types of approved lists: URL and file name. The list formats for each type is described below.

Note: Approved lists using the [approved] format cannot be imported. Blocked and allowed lists using the [blocked] and [allowed] formats can be imported.

Approved URL List Format

An approved URL list can be any ASCII text file containing the header:

[approved]

There is no limit to the number of URLs you can include in an approved list. Delimit separate Web addresses, URLs, and/or strings using a line break. Approved-lists support the following * and ? wildcards.

Sample file:

```
[approved]
www.good-job-habits.com/*
www.business-productivity.com/*
```

File Name List Format

A file name approved List can be any ASCII text file containing the header:

[approved]

There is no limit to the number of file names you can include in an approved list. Delimit separate file names and/or strings using a line break. Approved-lists support the * wildcard.

Sample file:

```
[approved]

abcfile.doc

*.sc
```

Setting the Scan Action for Viruses

After configuring the HTTP virus scanning rules, configure the actions that IWSVA takes if an infected file, uncleanable file, password-protected or macro-containing file is detected.

Scan Actions

There are four actions that IWSVA can take in response to the outcome of virus scanning:

- Choose **Delete** to delete an infected file at the server. The requesting client will not receive the file. This action can be applied to the *Infected files*, *Uncleanable files*, and *Password-protected files* scan events.
- Choose **Quarantine** to move a file (without cleaning) to the quarantine directory.

  ```
  /var/iwss/quarantine
  ```

  The requesting client will not receive the file. This scan action can be applied to all four of the scan events. You can optionally choose to encrypt files before sending them to the quarantine directory. For more information, see Quarantined File Handling starting on page 7-34.

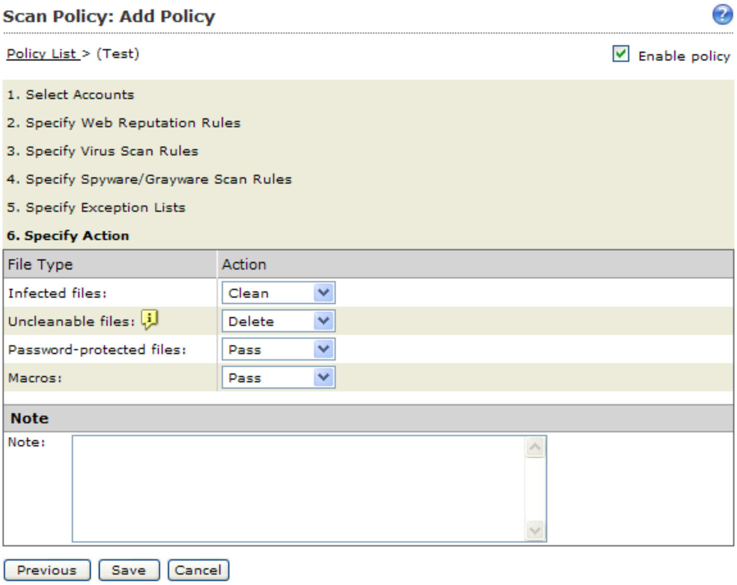
- Choose **Clean** to have IWSVA automatically clean and process infected files. The requesting client receives the cleaned file if it is cleanable, otherwise the uncleanable action is taken. This action can be applied to the *Infected files* and *Macros* scan events. For macro-containing files, the Clean action strips the macro from the file, whether the macro is a virus or benign, to protect your network before an updated virus pattern is released and deployed.
- Choose **Pass** to send the file to the requesting user. This action can be applied to the *Uncleanable files*, *Password-protected files*, and *Macros* events. The Pass action should always be used for Macros events, unless you want to strip or quarantine all macro-containing files during a virus outbreak.

Note: Trend Micro does not recommend choosing the *Pass* scan action for uncleanable files.

Scan Events

After scanning, you can configure actions for the four possible scanning outcomes:

- **Infected files**—Files determined to be infected with a virus or other malicious code. Available actions are **Delete**, **Quarantine** or **Clean** (recommended and default action).
- **Uncleanable files**—Depending on the type of virus or malicious code infecting a file, the scan engine might not be able to clean some files. Available actions are **Delete** (recommended and default action), **Quarantine**, and **Pass**.
- **Password-protected files**—Files that cannot be scanned because they are either password-protected or encrypted. The infection status of these types of files cannot be determined. Available actions are **Delete**, **Quarantine**, and **Pass** (recommended and default action).
- **Macros**—Microsoft Office files that contain macro program code. Because many of the fastest spreading viruses are macro viruses, you can quarantine all macro-containing files during the early stages of a virus outbreak to block all files before the new virus pattern is added to the pattern file and deployed to your environment. Available actions are **Quarantine**, **Clean**, and **Pass**. Unless there is a need to quarantine or strip macros during a virus outbreak before an updated pattern file is released, the action for Macro should always be set to **Pass**.



Scan Policy: Add Policy

Policy List > (Test) ☑ Enable policy

1. Select Accounts
2. Specify Web Reputation Rules
3. Specify Virus Scan Rules
4. Specify Spyware/Grayware Scan Rules
5. Specify Exception Lists
6. **Specify Action**

File Type	Action
Infected files:	Clean
Uncleanable files:	Delete
Password-protected files:	Pass
Macros:	Pass

Note

Note:

FIGURE 7-11. HTTP Virus Scanning Policy Action Configuration

Adding Notes to Your Policy

To record notes about your policy, type them into the **Note** field at the bottom after configuring the actions taken against files detected by IWSVA.

When you have completed configuring the scan actions to apply to your policy, click **Save**. Click **Deploy Policies** to immediately apply the policy; otherwise, the policy is applied after the database cache expires.

IntelliTunnel Security

IWSVA uses IntelliTunnel technology to block undesirable instant messaging (IM) and authentication connection protocols tunneled through port 80. It uses a dynamic, updatable pattern file to distinguish normal browser traffic from other protocols communicating over port 80. Currently, the pattern file can identify three popular types of IM traffic when this traffic is tunneled through port 80.

Because IWSVA is an HTTP/FTP proxy, it can only scan traffic that is submitted to it directly (through a browser's proxy setting), or through a network device (in bridge and ICAP modes). This means that IWSVA is only able to intercept HTTP (port 80), HTTPS (port 443), and FTP (port 21) traffic. Traffic to other ports are not routed through IWSVA and, thus, cannot be blocked by it. To ensure that IM traffic is routed through IWSVA, the clients must be configured to use HTTP tunneling with IWSVA because the proxy and outbound access through all other ports must be disabled at the firewall.

This section describes the protocols used for IM and authentication connections. It also describes how to edit and create an IntelliTunnel policy.

Note: IWSVA does not support IntelliTunnel in bridge mode.

Protocols Used in Instant Messaging and Authentication Connections

IWSVA can filter HTTP traffic for IM protocols and authentication connections protocols and, based on a specified policy, block certain content from entering the LAN. You can create multiple policies to have IWSVA apply different filter criteria to different user groups within your organization.

Policy enforcement is only possible when the IM clients are forced to use HTTP tunneling. This requires configuring the site to allow only external network access through HTTP. This means internal clients are prevented from connecting directly to external servers of any form, on any port. This is part of the firewall configuration, not IWSVA.

About Instant Messenger Protocol

IWSVA can currently block IM services using current commercial instant messenger protocols, including OSCAR (AIM and ICQ), MSNP (Microsoft Messenger), and YMSG (Yahoo Messenger).

About Authentication Connections

IWSVA can block authentication attempts for Google Talk, Jabber IM (using jabber.org as the authenticator), AIM, and ICQ.

Note: Because of the way that Google authenticates users, the Gmail application uses the same authentication as the Google Talk product. This means that blocking Google Talk also blocks Gmail.

IntelliTunnel cannot, however, block authentication connections in ICAP mode.

Editing an IntelliTunnel Policy

When editing a policy, you can edit the account information, policy information, or both.

To edit IntelliTunnel policy information:

1. Select **HTTP > IntelliTunnel** from the main menu.
2. Click the desired policy name.
3. From the **IntelliTunnel: Edit Policy** page (Rule tab), select or clear the appropriate option(s).
4. Click **Save**.

To edit IntelliTunnel account information:

5. Click the **Account** tab.

   You can also access the **Account** tab by clicking on the desired account name on the IntelliTunnel Policies page.
6. Specify a policy name.
7. Specify an IP range and/or an IP address and then click **Add**.

   IWSVA applies the IM and authentication connections rules to any IP range and IP address that you specify. If you are using LDAP, then you might see more descriptive information in the Add table, such as the user name.
8. Click **Save**.

Creating a New IntelliTunnel Policy

Creating a new IntelliTunnel policy is a two-step process: specify an account and specify IM/authentication connections security rules.

To create a new IntelliTunnel policy:

1. Select **HTTP > IntelliTunnel** from the main menu.
2. On the IntelliTunnel Policies page, click the **Add** link.
3. From the "1. Select Accounts" view of the IntelliTunnel: Add Policy page, specify a policy name.
4. Specify an IP range and/or an IP address and then click **Add**.

   IWSVA applies the IM and authentication connections rules to any IP range and IP address you specify. If you are using LDAP, you might see more descriptive information in the Add table, such as the user name.
5. Click **Next**.
6. From the "2. Specify IntelliTunnel Security Rules" view of the IntelliTunnel: **Add Policy** page, select the desired option(s).

   See the IWSVA online help for a complete description of the IM and authentication connections protocols.
7. Click **Finish**.

Java Applet and ActiveX Security

IWSVA Applets and ActiveX scanning blocks malicious Java applets and unsecured ActiveX controls at the Internet gateway, preventing them from infiltrating your network and performing malicious acts on client workstations.

IWSVA employs a tiered technology approach that operates on both the Internet gateway server and on desktops.

- On the server, IWSVA prefilters Java applets and ActiveX controls based on whether they are digitally signed, the validity of the signature, and the status of the certificates used to do the signing.
- On client workstations, IWSVA code, inserted into Java applets, monitors the behavior of the applets in real time and determines whether their behavior is malicious according to a pre-configured security policy.

Figure 7-12 illustrates how IWSVA scans and blocks malicious applets and ActiveX objects.

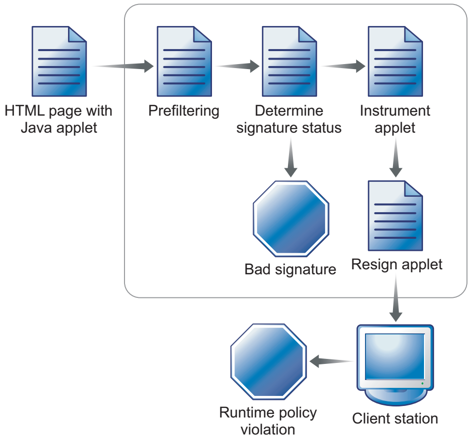


FIGURE 7-12. How Java applet security works

How Applets and ActiveX Security Works

As applets and ActiveX objects pass through the gateway, the validity of their digital signatures are checked. In addition, IWSVA monitors applets in real-time on the client workstations and issues an alert if any prohibited operations are attempted.

Step 1. Filtering Applets & ActiveX at the Server

As Java applets and ActiveX controls are downloaded to the proxy server, IWSVA filters them according to the following criteria:

For ActiveX Objects

If ActiveX security is enabled, IWSVA checks the signatures of CAB files and executable COM objects (of which ActiveX controls are a type) that are digitally signed. It then examines the digital certificates contained in the signature and compare them with those in the IWSVA-specific certificate database. ActiveX objects not signed, invalidly signed, or signed using an unknown root Certification Authority (CA) certificate can be blocked. In their place, the system creates a new HTML page containing a warning message. This new page is then delivered to client workstations.

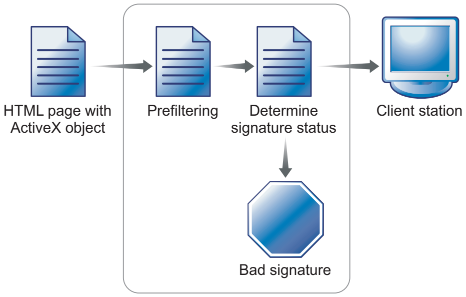


FIGURE 7-13. How ActiveX Security Works

For Java Applets

IWSVA filters Java applets based on whether they are digitally signed, the validity of the signature, and the status of the certificates used to do the signing.

If signature verification is enabled, IWSVA verifies the signatures of digitally signed applets. Those not signed, signed using an unknown or inactive root Certification Authority (CA) certificate, signed using a flagged certificate, or invalidly signed can be blocked. They are then replaced with a new applet that displays a warning message. If certificate checking is disabled, the system accepts all Java applets regardless of the certificates they carry.

IWSVA keeps a database of recognized certificates, which is used in the filtering process. This database is automatically updated to include any unrecognized certificate the system encounters. You can delete entries from the database and enable or disable entries on the **HTTP > Applets and ActiveX > Manage Digital Certificates** screen (see Managing Digital Certificates starting on page 7-62).

For Java Applets, IWSVA first performs Steps 2 and 3 below before sending the applets to the clients.

Step 2. Instrumenting Applets

IWSVA analyzes the applet code to determine any potentially dangerous actions that it might perform. It then adds instrumentation code (that is, instructions that notify the user of certain programming operations) to monitor and control these actions.

During instrumentation, IWSVA inserts monitoring code around suspicious instructions and then attaches the security policy assigned to the intended recipients. Depending on how IWSVA is configured, this security policy might vary from one client to another, based on the domain they belong to or their IP addresses. IWSVA supports creating multiple policies that can be mapped to different groups of users in your network. IWSVA uses the inserted monitoring codes and the attached security policy to monitor the applet's behavior in real-time and to determine whether or not this behavior is malicious.

Note: The process of instrumenting a signed applet renders the signature invalid. Therefore, the signature is stripped, leaving it unsigned. IWSVA can optionally re-sign the applet if required by the client browser.

Step 3. Optionally Re-signing Instrumented Applets

If configured to do so, IWSVA re-signs the instrumented applets using an imported "private key" before sending them to client workstations. Because applets lose their original signatures during the instrumentation process (due to modifications to their original code), you might want to use this feature to ensure that the clients' Web browsers run the instrumented applets with the permissions they might require to run correctly.

IWSVA supports the import of a "private key", along with the associated certificate that contains the corresponding "public key," for use in the re-signing process. You can purchase this key from any of the well-known Certifying Authorities (CAs). Only one re-signing key may be configured for use at any given time.

Note: Re-signing applies only to validly signed applets. If the system is configured to accept unsigned applets, these applets bypass this process and are delivered to client workstations immediately after instrumentation.

Step 4. Monitoring Instrumented Applet Behavior

When the applet executes in the browser, the instrumentation is automatically invoked before any potentially dangerous operation is performed. The instrumentation determines whether an action is permitted by comparing it with the attached security policy. If the action is permitted, IWSVA then allows the action to take place; otherwise, IWSVA notifies the users and gives them the option to allow the behavior, terminate the behavior, or stop the applet.

Enabling Applet/ActiveX Security

To start scanning your HTTP traffic for malicious applets and ActiveX objects, enable this scanning from the Applets and ActiveX policy page.

To enable malicious Applets and ActiveX scanning in HTTP traffic:

1. Select **HTTP > Applets and ActiveX > Policies** from the main menu.
2. Check **Enable Applet/ActiveX security**.
3. Click **Save**.

Adding and Modifying Applet/ActiveX Scanning Policies

The first step when configuring a new policy is to set the client accounts to which the policy applies. See Configuring the Scope of a Policy starting on page 6-22 for more information and procedures for setting a policy's scope using the three different user identification methods.

All configured policies are listed on the **Applets and ActiveX Policies** screen available from **HTTP > Applets and ActiveX > Policies**.

To modify the scope of a policy:

1. Open the **Applets and ActiveX Policy** screen (**HTTP > Applets and ActiveX > Policies** from the main menu).
2. Do one of the following:
   - To remove accounts from a policy's scope, select the users, click **Delete** and then **Save**.

  - To add accounts to a policy's scope, click the **Policy Name**, switch to the **Account** tab, add or delete the accounts to which the policy applies, and click **Save**.

3. Click **Deploy Policies**. Changes to a policy's scope do not take effect until the modified policies are deployed.

After configuring the scope of your policies, configure the applet and ActiveX scanning rules.

Configuring Java Applet Security Rules

On the **HTTP > Applets and ActiveX > Policies** screen, add a new policy or select an existing policy. On the **Java Applets Security Rules** tab, IWSVA can be configured to either block all applets, or to accept and process applets using the security settings you specify.

Signature Status

A digital signature is a way to verify the genuine publisher of an applet. It also allows you to verify that the applet has not been tampered with or otherwise changed because it was published. After analyzing the applet's signature, IWSVA makes one of the following determinations:

- **Valid signature**
- **No signature:** The applet is unsigned.
- **Invalid signature:** The applet's signature is corrupt or cannot be verified for some reason; for example, no trusted root certificate is found

Checking the signature of an applet is done in two steps. The first verifies the integrity of the applet code against data in the signature. The second verifies the integrity of the certificates, the "certificate chain," used to create the signature. For the signature to be considered valid, the certificate chain must end with a trusted certificate recognized by IWSVA. The set of these certificates can be viewed and managed by opening the Web console to **HTTP > Configuration > Digital Certificates > Active Certificates**.

Certificate Status

Java applet security rules can apply different actions to applets that have valid signatures, based on their certificate status.

By default, IWSVA trusts its active certificates. However, an active certificate can be "flagged" if you no longer want to trust applets that have a flagged certificate in their certificate chain. Flagged certificates continue to be listed as active certificates, though the flagged status is noted.

Instrumentation and Re-signing

Instrumentation is the process through which IWSVA adds monitoring and control code to the applet. Because the instrumentation process breaks the applet's signature, if any, you can alternatively choose to re-sign an applet after instrumentation. This ensures the instrumented applets executes in the browser and perform operations as expected.

Applet Instrumentation Settings

The purpose of instrumenting applets is to prevent applets from executing prohibited operations on client machines. By default, Java applets processed by IWSVA are not allowed to perform the following types of operations:

- **Destructive operations:** Deleting and renaming files
- **Non-destructive operations:** Listing files in a directory or retrieving file attribute information
- **Write:** Writing new or modifying existing files
- **Read:** Reading file contents

Configuring Exceptions

For each of the types of operations that can be selectively allowed or prohibited, you can configure file or folder exceptions where the security policies do not apply.

- To allow a given type of file operation, except when performed by a subset of files, check the **Enable** button next to the file operation. Click the **Exceptions** link. The **Exceptions to File Operations** screen opens. Configure the files and folders where the operation is not allowed.

- To disallow a given type of file operation, except for a subset of files, check the **Disable** button next to the file operation. Click the **Exceptions** link and then configure the files and folders where the operation is allowed.

To configure Java applet processing settings:

1. After setting the scope of your policy, do one of the following:
   - Select **Process Java applets using the following settings** for IWSVA to pass, block or instrument the applet based on its signature and certificate status.
   - Select **Block all Java applets** for IWSVA to not allow any applets to pass to the clients. If you choose this setting, proceed to step Step 3.
2. For each of the following signature and certificate status, choose the processing action to use (* denotes the default Trend Micro-recommended settings):
   - **Valid signature, trusted certificate**: Pass*, Instrument applet (re-sign), Instrument applet (strip signature), Block
   - **Valid signature, flagged certificate**: Pass, Instrument applet (re-sign), Instrument applet (strip signature), Block*
   - **No signature**: Pass, Instrument Applet*, Block
   - **Invalid signature**: Pass, Instrument Applet (strip signature), Block*
3. For each of the four (destructive, non-destructive, write or read) operations that can be selectively enabled or disabled, click **Enable** or **Disable** to configure your security policy.
4. Click **Exceptions**, and then configure the files or folders that are exceptions to the security policy:

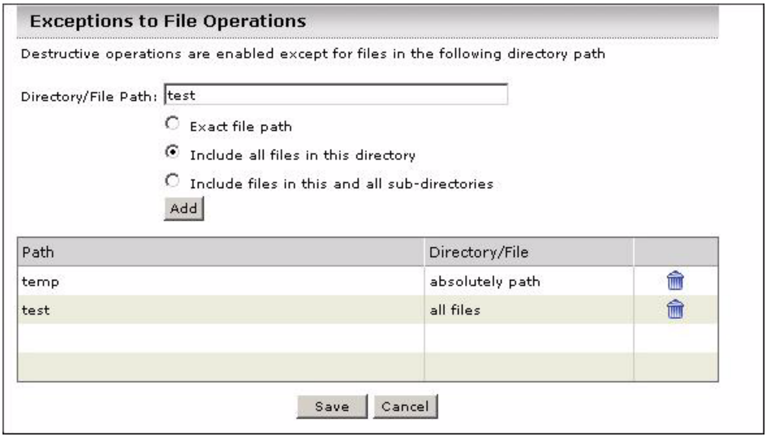
   a. Enter the **Directory/File Path** of the files that do not apply to the configured security policy.
      - To configure a specific file path, select **Exact file path**.
      - To exclude the entire folder's contents from the security rule, select **Include all files in this directory**.
      - To exclude all of the folder's files, plus those in subdirectories, from the security rule, select **Include files in this and all subdirectories**.

Note: All file paths are those on the client machine, where the applet runs. The file path format should be in the form required by the operating system running on the client.

b. Click **Add** to add the exceptions to the given security policy.

c. Configure other files or directories to exempt from the applet's security settings.

d. When you've completed configuring your file and folder exceptions, click **Save**.



Exceptions to File Operations

Destructive operations are enabled except for files in the following directory path

Directory/File Path: test

○ Exact file path

● Include all files in this directory

○ Include files in this and all sub-directories

Path	Directory/File	
temp	absolutely path	🗑
test	all files	🗑

FIGURE 7-14. Java applet instrumentation settings exception files and folders

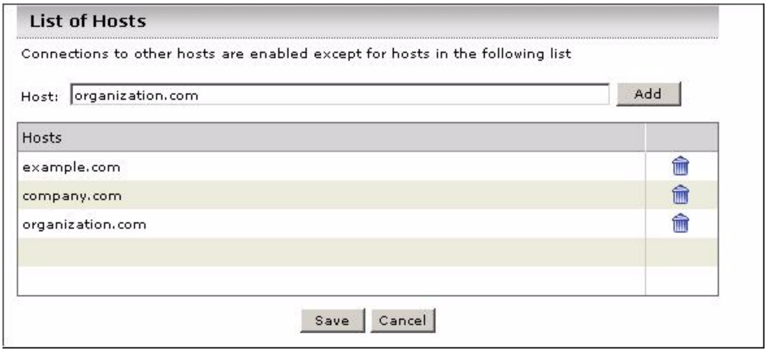
5. On the **Java Applet Security Rules** tab, select **Bind local ports** to allow applets to bind to ports on the client workstation.
6. To allow applets to connect to their originating servers, select **Connect to their originating servers**.
7. To allow applets to connect to hosts other than the ones they originated from, select **Enable** or **Disable** next to **Host connections**, then configure exceptions to the security policy.

   a. Enter the **Host** that does not apply to the configured security policy.

   b. Click **Add** to add the exceptions to the given security policy.

c. Add others host that do not apply to the security policy.

d. When you've completed configuring the hosts that are exceptions to the policy's security rules, click **Save**.



List of Hosts

Connections to other hosts are enabled except for hosts in the following list

Host: organization.com

Hosts
example.com
company.com
organization.com

FIGURE 7-15. Exceptions to the Java applet host connection rules

8. Select **Create new thread groups** to allow applets to create new thread groups. To disallow this operation, clear it.
9. Select **Create unlimited active threads** to have IWSVA ignore thread activity from applets downloaded to clients on the LAN and specify a limit to restrict the number of threads applets can create at one time. To disallow this operation, clear it.
10. Select **Create unlimited active windows** to limit the number of active top-level windows applets can open. Enter the number of allowable windows in the provided text box. Clearing this option gives applets the freedom to open as many windows as they want—just like some malicious Java applets do to annoy users.
11. Enter any optional **Note** for future reference about this policy.
12. Click **Next** to continue with configure ActiveX security rules if you are configuring a new Applets and ActiveX policy. If you are modifying an existing policy, click **Save**.
13. Click **Deploy Policies** to immediately apply the policy; otherwise, the policy is applied after the database cache expires.
14. Enter any notes to save pertinent information about this policy, and then click **Save**.

Configuring ActiveX Security Rules

ActiveX security rules can be applied to the two different types of ActiveX controls:

- **Executable cabinet files** (*.cab): An ActiveX control distributed using the Windows native compressed archive format.
- **Portable executable (PE) files** (*.exe, *.ocx, and so on): An executable file format that has “portability” across all 32-bit and 64-bit versions of Windows.

For each of these two file types, you can configure security policies to:

- Block all ActiveX controls of that type
- Allow all ActiveX controls of that type
- Verify signatures, and alternatively block invalidly signed or unsigned files

Enter any notes about this policy and then click **Save**.

Applying Applet and ActiveX Policy Exceptions

There may be URLs or Web sites that you want exempt from an Applet and ActiveX policy (for example, the corporate intranet, business partner sites, and research tool sites).

In the **Exceptions** tab, select the name of the approved URL list to be exempted from the **Approved URL List** field.

You can create exception lists in the **HTTP > Configuration > Approved Lists** page (see *Specifying the Exception Lists* on page 7-38 for more information).

Applet and ActiveX Settings

Applet and ActiveX security policies determine certificate and signature status as configured on the **Applet and ActiveX Settings** page. For example, IWSVA can either attempt to validate signatures, strip the signatures and process all applets as being unsigned, or check the certificate’s revocation status. In addition, IWSVA can re-sign applets after instrumentation.

To validate the signature of an ActiveX control, IWSVA can check the expiration of the signing certificate, check all certificates in the signing chain (exclusive of the signing certificate) and check the revocation status of the certificate (where a revocation information source is available for a certificate).

To configure how IWSVA validates Java applet and ActiveX signatures:

1. Click **HTTP > Applets and ActiveX > Settings** from the main menu.
2. Complete the settings on the **Java Applets** and **ActiveX Executable**s tabs.
3. Click **Save**.

Java Applet Signature Validation

When IWSVA processes signed applets, it can handle digital signatures in one of two ways:

- Strip signatures and treat all incoming applets as unsigned applets, a restrictive security setting that treats all applets, signed or unsigned, in the same manner. In a normal client browser environment, the unsigned applet does not have access to the client system's resources, but it can still produce annoying behavior such as opening many windows.
- Perform full signature validation on the applets.

Adding Certificates for Applet Signature Verification

Java applet signatures are verified using root certificates installed. To see the list of root certificates, select **HTTP > Configuration > Digital Certificates** from the main menu. ActiveX signatures are verified against the root certificates in the IWSVA device's Windows certificate store.

If your environment requires running applets signed with root certificates that are not installed along with IWSVA, then add them to the IWSVA digital certificate store.

To add a certificate to the IWSVA certificate store:

1. Click **HTTP > Configuration > Digital Certificates** from the main menu.
2. On the **Active Certificates** tab, click **Add**, select the certificate, and then click **Add**.
3. Return to the **Active Certificates** screen and verify that the added certificate appears on the list.

Certificate Expiration

IWSVA can be configured to:

- Check that the certificate used to sign the applet has not expired
- Check that the certificates in the certification path are all valid

Untrusted Signature Status

If IWSVA is unable to determine whether the certificate should be trusted because of its certification path, then the applet's signature status can be set to:

- Unsigned (which means the signature is stripped), or
- Invalid

Revocation Status

Digital certificates can be revoked by their issuer. IWSVA can check whether a certificate has been revoked when a status source is available.

If IWSVA cannot access the defined status source, you can configure IWSVA to set the status of the certificate to Valid, Unsigned (Strip signature), or Invalid.

Applet Re-signing

IWSVA can re-sign instrumented applets with your company's own "private key" before they are sent to client workstations. Because applets lose their original certificates during instrumentation, you might want to re-sign them to ensure that clients' Web browsers always accept the applets without any restrictions.

To use the re-signing feature, you need two keys: 1) a "private key" that must be imported into IWSVA, and 2) a certificate containing the "public key" equivalent to your "private key" that must be imported into your clients' Web browsers. The certificate enables the browsers to recognize the signature you affix to instrumented applets. Without this certificate, these applets are treated as another unsigned applet—either blocked by the browser or given limited access to system resources.

IWSVA supports the PKCS12 key format. If you do not have a key yet, you can purchase one from any of the well-known Certificate Authorities (CAs).

To re-sign applets after instrumentation:

1. On the **Java Applets** tab of the **Applet and ActiveX Settings** page (**HTTP > Applets and ActiveX Settings**), check **Re-sign the applets with the following certificate**.
2. Type the path or click **Browse** to navigate to the certificate to use for re-signing.
3. Enter the certificate's **Password**.
4. Click **Add**.
5. Click **Save**.

ActiveX Signature Validation

To verify whether an ActiveX control is validly signed, IWSVA can check the control's certificate in several ways—for both a Cab file and PE file. This validation includes checking the expiration of the signing certificate, the expiration of all certificates in the signing chain, or by checking the revocation status of the certificate (when a status source is defined).

To configure how IWSVA checks the signature status of a signed ActiveX control:

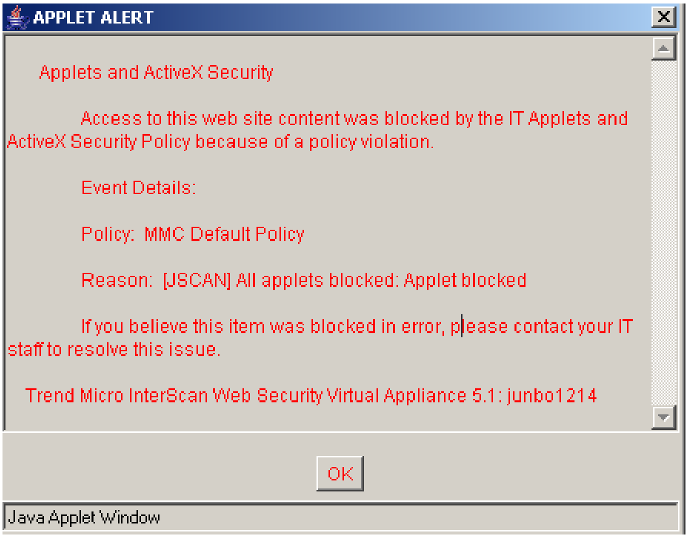
1. Select **HTTP > Applets and ActiveX > Settings** from the main menu, and click the **ActiveX Executables** tab.
2. Enable the types of signature checking to use for ActiveX controls:
   - Verify that the signing certificate has not expired
   - Check that all of the certificates in the certifying path have not expired
   - When the certificate's issuer is defined, verify whether the certificate has been revoked by the issuer
   - Signature timestamps can be checked. If set, a signature with an expired certificate is considered valid if it has a valid timestamp counter-signature.

   If IWSVA is unable to access the certificate's issuer, then the status of the signature can be set to either **Valid** or **Invalid**.
3. Click **Save**.

Client-side Applet Security Notifications

There are several alert messages that might be displayed in the client's browser in response to IWSVA Java applet security policies.

If an applet is blocked due to its signature or certificate status, the requesting client is presented with a message showing the policy that blocked the applet, along with the reason:



APPLET ALERT

Applets and ActiveX Security

Access to this web site content was blocked by the IT Applets and ActiveX Security Policy because of a policy violation.

Event Details:

Policy: MMC Default Policy

Reason: [JSCAN] All applets blocked: Applet blocked

If you believe this item was blocked in error, please contact your IT staff to resolve this issue.

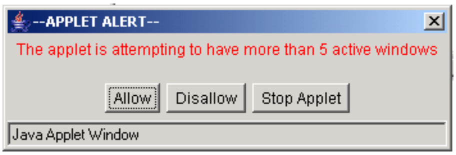
Trend Micro InterScan Web Security Virtual Appliance 5.1: junbo1214

FIGURE 7-16. Blocked applet notification

If an instrumented applet attempts to perform an operation that is not allowed by a policy's configuration, a notification displays the disallowed operation and the user is prompted on how to proceed. Available options are:

- **Allow**: The instrumented applet continues to run, including the operations not allowed by the policy.
- **Disallow**: The operation that triggered the Applet security policy is stopped, but the instrumented applet continues to run.

- **Stop Applet**: The instrumented applet is terminated.

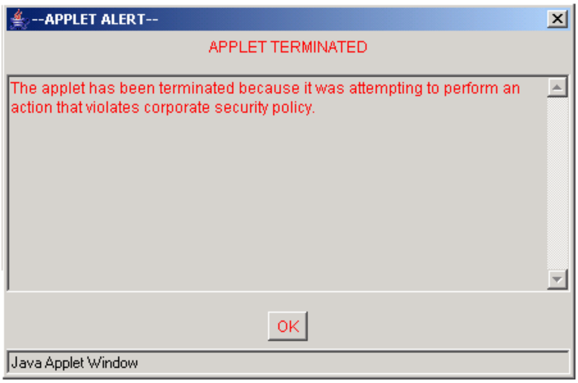


--APPLET ALERT--

The applet is attempting to have more than 5 active windows

FIGURE 7-17. Applet Security Violation Notification

If the client chooses **Stop Applet**, another notification is displayed to indicate that the applet has terminated.



--APPLET ALERT--

APPLET TERMINATED

The applet has been terminated because it was attempting to perform an action that violates corporate security policy.

FIGURE 7-18. Applet Execution Termination Notification

Managing Digital Certificates

For IWSVA to determine that a Web server's or an applet's signature is trusted, the root Certification Authority (CA) certificate on which the signature is based must be added to the IWSVA certificate store.

There are three types of digital certificates that are involved in producing a digital signature:

- The "end" or "signing" certificate, which contains the public key to be used to validate the actual applet signature

- One or more "intermediate" Certification Authority (CA) certificates, which contain the public keys to validate the signing certificate or another intermediate certificate in the chain
- The "root" CA certificate, which contains the public key used to validate the first intermediate CA certificate in the chain (or, rarely, the signing certificate directly). An otherwise valid signature is "trusted" by IWSVA if the CA certificate of the signature is known to IWSVA, is active, and is not flagged.

If IWSVA encounters an unknown certificate during SSL handshake or applet signature processing, it saves the certificate in the "inactive" list, along with the URL of the Web site or applet that contained the signature. All types of certificates are collected in this way (signing, intermediate, and root). If required later, a CA certificate collected this way can be "activated" (made trusted by IWSVA) so that the signatures of applets that depend on it can be processed as valid. Intermediate CA and end certificates might be activated, but this only has an effect if the root certificate is also activated. In other words, activating an intermediate CA or signing certificate does not make them trusted (only CA certificates can be made trusted), but any certificate might be flagged.

To manage the certificates in the IWSVA certificate store, you can perform the following operations:

- **Delete a certificate:** Removes the selected certificate(s) from the certificate store.
- **De-activate a certificate:** Keep the certificate in the IWSVA certificate store, but do not trust certificates that use it in their certification path.
- **Activate a certificate:** Make a CA certificate trusted.
- **Flag the certificate:** Flag all signatures that use the certificate in its certification path.
- **Clear flagged certificate:** Re-instate the trusted status of a certificate that was previously flagged, so that certificates that use the certificate in their certification path is trusted.

To view existing certificates:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Switch between the **Active Certificates** and **Inactive Certificates** tabs to see which certificates are already known to IWSVA.

To add a trusted certificate:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Ensure the **Active Certificates** tab is active.
3. Click **Add**.

   The **Add Certificates** screen opens.
4. Type the path or click **Browse** to navigate to the certificate to add and click **Add**.

   Note: Certificates are commonly contained in files with the extensions .cer, .der, .crt. Also, only active CA certificates are considered trusted, but any active certificate might be flagged.

   The screen returns to the **Active Certificates** tab. The certificate that you added should be visible, along with the type of certificate and its expiration date.

To delete a certificate:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Select the certificate(s) to delete.
3. Click **Delete**.

To de-activate a trusted certificate:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Make sure the **Active Certificates** tab is active.
3. Check the certificate(s) to de-activate.
4. Click **De-activate**.
5. The certificate(s) that you selected moves to the **Inactive Certificates** tab.

To activate a certificate:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Make sure the **Inactive Certificates** tab is active.
3. Select the certificate(s) to activate.
4. Click **Activate**.
5. The certificate(s) that you selected moves to the **Active Certificates** tab.

To flag a certificate:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Make sure the **Active Certificates** tab is active.
3. Select the certificate(s) to flag.
4. Click **Flag Certificate**.
5. The flagged certificate(s) remains visible on the **Active Certificates** tab, with a red flag in the status column.

To remove a certificate from being flagged:

1. Select **HTTP > Configuration > Digital Certificates** from the main menu.
2. Make sure the **Active Certificates** tab is active.
3. Select the flagged certificate(s) to be cleared (certificates with flagged status have a red flag in the **Status** column).
4. Click **Clear Flagged Certificate**.
5. The flagged certificate(s) remains visible on the **Active Certificates** tab, without a red flag in the **Status** column.

Chapter 8

Access Quotas and URL Access Control

Access quotas limit a client's bandwidth consumption to a fixed amount per unit of time. URL trusting can improve browsing performance by exempting trusted URLs from scanning and other InterScan Web Security Virtual Appliance (IWSVA) operations. URL blocking refuses requests to URLs that you specify or whose patterns are contained in the Phish pattern file.

Topics in this chapter include:

Introduction to Access Quota Policies

The InterScan Web Security Virtual Appliance access quotas Guest Policy limits the HTTP bandwidth used by clients who access the Internet through the InterScan Web Security Virtual Appliance guest port. A policy for other clients can also be defined (there is no access quota Global Policy). If no policy matches the connection, then the client has unlimited access. After modifying access quota policies and saving the policies to the database, the InterScan Web Security Virtual Appliance service in a multiple server configuration environment reloads the policies according to the time-to-live (TTL) value configured in the **HTTP Configuration** screen (**Administration > IWSVA Configuration > Policy Deployment**.)

If the quota is exceeded while making a download, the download is allowed to continue. However, succeeding downloads/browsing requests (before the access quota interval expires) are refused. Users are allowed access again after the access quota interval expires.

Note: For a group quota policy, the quota is for each client within the policy's scope, and all clients in the same policy have the same quota.

Managing Access Quota Policies

The clients within the scope of an access quota policy, the bandwidth quota and the time interval for the quota's duration are configurable.

To add an access quota policy:

1. Click **HTTP > Access Quota Policies** from the main menu.
2. Select **Enable access quota control**.
3. From the drop-down menu, select the access quota interval—either **Daily**, **Weekly**, or **Monthly**.

   The value for the access quota interval is globally applied to all access quota policies, including all existing policies.
4. Click **Save**.
5. Click **Add**.
6. Select **Enable policy** and enter the access quota.

7. Select the users to which the policy applies.

   The options on this page depend upon the user identification method that you are using—either *IP address*, *Host name (modified HTTP headers)*, or *User/group name authentication*. These settings are configured in the **HTTP > Configuration > User Identification | User Identification** tab. For more information about configuring the user identification method and defining the scope of a policy, see Configuring the User Identification Method starting on page 6-5.

   Regardless of the user identification method you have configured, you can always enter IP addresses of the clients to which the policy applies.

8. Type some optional notes to record any special information about the policy.
9. Click **Save**.
10. When returned to the **Access Quota Policies** page, click **Deploy Policies** to immediately apply the policy; otherwise, the policy is applied after the database cache expires.

There might be occasions when you want to temporarily deactivate a policy, without deleting the settings from the database.

To deactivate a policy:

1. Click **HTTP > Access Quota Policies** from the main menu.
2. From the **Access Quota Policies** screen, click the linked item in either the **Account** or **Access quota** column to go to the Edit Policy screen.
3. Clear **Enable policy** at the top of the screen and then click **Save**.

   Disabling the policy does not take effect until the policy cache refreshes, or you click **Deploy Policies**.

If you no longer have any need for a policy (for example, if the employee using the client leaves your organization), you can either delete the whole policy or users within the policy's scope from the InterScan Web Security Virtual Appliance database.

To delete a policy:

1. Click **HTTP > Access Quota Policies** from the main menu.
2. From the **Access Quota Policies** screen, select the policy and then click **Delete**.

   Deleting the policy does not take effect until the policy cache refreshes, or you click **Deploy Policies**.

Overview of URL Access Control

IWSVA can control a URL's access based on Web Reputation feedback, the URL Filtering module, or a combination of both. The combination of Web Reputation and the URL Filtering module is a multi-layered, multi-threat protection solution provided by IWSVA.

The URL Filtering module grants or denies Web access based on the category to which a URL belongs. Web Reputation grants or denies Web access based on whether the requested URL is a phishing or pharming threat that has hacking potential, or has a reputation score that deems it untrustworthy. Both the URL Filtering module and Web Reputation are controlled by the specifications you make in policies.

When a user attempts to access a Web site, the following events occur:

- IWSVA checks the requested URL against the URL blocking list and trusted URL list (see Overview of URL Access Control on page 8-4).

  If the URL is found on the URL blocking list, the request is denied. If the URL is found on the URL trusted list, access is granted and no form of access control is done.

- If the URL is not on the blocked or trusted list, IWSVA sends the requested URL to Web Reputation for processing.
- From a remote database, Web Reputation retrieves the appropriate URL rating for the URL.

  The rating can either be "high," "medium," or "low." The sensitivity level you specify determines whether or not IWSVA blocks the URL (see Specifying Web Reputation Rules on page 7-13).

  If the URL is found on an approved list, IWSVA skips the anti-phishing and anti-pharming detection for this URL (see Specifying the Exception Lists on page 7-38).

- Web Reputation then determines if the requested URL is a phishing or pharming threat and if so, flags the URL accordingly (see Anti-phishing and Anti-pharming Detection on page 7-14).
- The final process of Web Reputation is to determine the category of the URL (see Direct URL Filter Category Selection on page 1-9).

  The category information is used later by the URL Filtering module.

- Web Reputation returns the URL rating to IWSVA, any phishing or pharming flags, and the URL category.
- If a URL is flagged for phishing or pharming, IWSVA blocks access to the Web site.
- Next, if you are using the URL Filtering module, this module uses the Web category information for the requested URL to determine if access is permissible.

  If the URL is found on the approved URL list, the URL bypasses the category filtering and proceeds to the final step in URL access control (see Work and Leisure Schedule Settings on page 9-11).

  If the category of the requested URL is permitted in the URL Filtering policy, then the URL is passed on to the final step; otherwise, the URL is blocked.
- Finally, based on the Web Reputation URL rating, IWSVA determines whether the requested URL is below or above the sensitivity level specified in the scan policy.

  If the URL is found on an approved list, IWSVA skips the sensitivity level checking for this URL (see Specifying the Exception Lists on page 7-38).

  If the rating falls below the sensitivity level, the requested URL is blocked. However, if the rating is above the sensitivity level, IWSVA grants access.

Specifying URL Access Control

InterScan Web Security Virtual Appliance can optionally “trust” some URLs and exempt them from scanning and filtering to improve browsing performance to low risk sites. It can also block access to sites using a user-configured list, or by checking requested sites against the Phish pattern file, a compilation of sites associated with “phishing” schemes or other malicious acts.

Configuring Trusted URLs

InterScan Web Security Virtual Appliance can be configured to trust some URLs and exempt them from scanning and filtering. Because this opens a security risk by allowing unchecked content into your network, configuring a URL as “trusted” must be considered carefully. Because trusted URLs are not scanned, browsing performance is improved. Good candidates for trusting are Web sites that are frequently accessed and contain content you can control (for example, your company’s intranet sites).

Trusted URL information is kept in the `[URL-trusting], normalLists` section of the `intscan.ini` configuration file.

When configuring trusted URLs, you can specify the sites using the following:

- The Web site, which includes any sub-sites
- Exact-match strings within a requested URL

You can apply exceptions to sites that would otherwise match the criteria for the trusted URL list, so InterScan Web Security Virtual Appliance scans or filters them as usual.

A list of trusted URLs and their exceptions can also be imported from a file, in addition to configuring them through the user interface. Write a comment or title (which InterScan Web Security Virtual Appliance ignores) at the top of a file that contains a list of Web sites, URL keywords, or strings, and then write one rule per line. Group sites to be blocked under `[block]` as shown in the following example, and group exceptions under `[allow]`:

```
URL Blocking Import File {this title is ignored}

[block]
www.blockedsite.com*
unwanted.com*
urlkeyword
banned.com/file
banned.com/downloads/

[allow]
www.blockedsite.com/file
www.unwanted.com/subsite/
www.trendmicro.com*
```

Note: For HTTPS decryption policies, the strings to match vary depending on whether you set IWSVA in proxy or transparency mode.
- In proxy mode, IWSVA matches the domain names, not the full URL. Thus, you only need to specify the domain names.
- In transparency mode (WCCP or bridge mode), IWSVA matches the CommonNames in the server certificates received.

Managing your trusted URLs and exceptions:

1. Click **HTTP > URL Access Control > Global Trusted URLs** from the main menu.
2. In the **Trusted URLs** configuration page, select **Enable Trusted URLs** to enable URL trusting.

   WARNING! **When you select the "Enable Trusted URLs" option, the content of trusted URLs will not be filtered and scanned for viruses.**

3. Select how you want to specify the URL to trust:
   - **Web site** match (including all sub-sites)
   - **String** match (URL must contain the string)
4. Type the URL string to **Match** and click **Trust** to add it to the Trusted URLs list (shown below the "**Do Not Scan these URLs**" section). To configure exceptions to the trusted URLs list, click **Do Not Trust** and your entry is entered under **Exceptions to the Trusted URL List**.
5. To remove a trusted URL or exception from your trusted URLs list, highlight the item and click **Remove**. **Remove All** clears all the items.
6. Click **Save**.

To import a list of trusted URLs and their exceptions:

1. Click **HTTP > URL Access Control > Global Trusted URLs** from the main menu.
2. Browse or type the name of the file that contains the list of trusted URLs and their exceptions into the "**Import Trusted list and exceptions**" field.
3. Click **Import**. The trusted URLs and their exceptions from the file appear in the appropriate fields on the interface.
4. Click **Save**.

Blocking URLs

InterScan Web Security Virtual Appliance can block Web sites and URL strings in the global blocked URL list.

Note: If you have installed the ICAP proxy handler, configure the ICAP client to scan files in pre-cache request mode to make this feature work.

Depending on the deployment mode, you can block an HTTPS Web site by entering the FQDN (in standalone/dependent mode) or certificate cn information (in bridge or WCCP mode).

When configuring URLs to block, you can specify the sites using the following:

- The Web site, which includes any sub-sites
- Keyword matching within a URL
- Exact-match strings within a requested URL

You can apply exceptions to the blocked URL list so InterScan Web Security Virtual Appliance allows requests as usual. Using this feature, you can block a given site to allow access to some of its sub-sites or files. The URL Blocking list (including exceptions) is maintained in the `/etc/iscan/URLB.ini` file. The path for the `URLB.ini` file is set using the "normalLists" parameter under the [URL-blocking] section in the `intscan.ini` file.

You can also block URLs based on pattern matching with the Phish pattern file (`/etc/iscan/URLB.ini`), a database of patterns of Web sites associated with phishing or related schemes.

In addition to adding the URLs through the Web console, URL block lists can be imported from a text file.

Using a Local List

You can configure InterScan Web Security Virtual Appliance to block access to URLs based on a list of blocked sites and exceptions that you maintain for your environment.

When adding URLs to the **Block List** and "**Exceptions to the Block List**," it is best that you first make all additions to one list and then save this configuration before you make additions to the other list. This method helps ensure that the same URL exists in both lists. If you attempt to add a URL to the **Block List** or **Exceptions to the Block List** and it already exists in the other list, InterScan Web Security Virtual Appliance prevents the addition and displays a warning message stating that the entry already exists in the other list.

To configure URLs to block:

1. Click **HTTP > URL Access Control > Global URL Blocking**.
2. Select "**Enable URL blocking**."
3. On the **Via Local List** tab, type the full Web address or URL keyword, or exact-match string in the **Match** field.

   To identify a folder or directory in a given Web site, use a forward slash (/) after the last character. For example, if you want to block `www.blockedsite.com` but allow access to its `charity` directory:

   a. Type `www.blockedsite.com` in the **Match** field, then click **Block**.

   b. Type `www.blockedsite.com/charity/` in the **Match** field, and click **Do Not Block**. (If you write `charity` without the forward slash, IWSVA considers `www.blockedsite.com/charity` as a file.)

   Note: For HTTPS decryption policies, the strings to match vary depending on whether you set IWSVA in proxy or transparency mode.
   - In proxy mode, IWSVA matches the domain names, not the full URL. Thus, you only need to specify the domain names.
   - In transparency mode (WCCP or bridge mode), IWSVA matches both the CommonNames and URLs. You must include these in the blocking list if you want to block an HTTPS site.

4. Click **Remove** to remove the highlighted entries from the list (or **Remove All** to remove all entries).
5. Click **Save**.

Importing a List of Blocked URLs from a File

InterScan Web Security Virtual Appliance can import a list of URLs to block from a file. Type a descriptive title or comment on the first line of a file that contains a list of Web sites, URL keywords, or strings, and then write one rule per line. Group sites to be blocked under `[block]` as shown in the example, and group exceptions under `[allow]`. For example:

```
URL Blocking Import File {this title will be ignored}

[block]
www.blockedsite.com*
unwanted.com*
urlkeyword
banned.com/file
banned.com/downloads/

[allow]
www.blockedsite.com/file
www.unwanted.com/subsite/
www.trendmicro.com*
```

To include the "*" and "?" characters in a URL blocking string rather than having IWSVA consider them as wildcards, use variable %2a or %2A to represent ***** and variable %3f or %3F to represent **?**. For example, to block `www.example.com/*wildcard` literally, specify the blocking rule as `www.example.com/%2awildcard` instead of `www.example.com/*wildcard`.

If importing the list is not successful, verify that you have followed the specified format for the URL Blocking import file before contacting customer support. Be sure you have:

- Listed blocked entries under `[block]` and exceptions under `[allow]`
- Formatted entries containing wildcards as described in this document or the online help

To import a list of URLs to block:

1. Format a text file as described above with the URLs to block, along with any exceptions.
2. Click **HTTP > URL Access Control > Global URL Blocking** from the main menu.

3. Specify the location of the file to import in the "**Import block list and exceptions"** field by clicking **Browse**, and clicking **Import**.
4. Click **Save**.

Using a Pattern File (Phish)

Phishing attacks use fake email messages to lure potential victims. "Phishers" imitate an email message from a company with whom the user has an account. These fraudulent email messages seem authentic, and many recipients are deceived into supplying their personal information, such as a credit card account number, eventually resulting in the user becoming a victim of computer crime.

Phish is a Trend Micro service that leverages the following:

- Ability of IWSVA to block outbound access to a specific URL
- Capability of the Trend Micro antivirus team to collect and analyze customer submissions and distribute a database of known harmful URLs.

Phish can minimize harm from private and confidential information from being sent out from the client. Phish also prevents access to known phishing URLs.

The URL that is determined to maliciously collect user information is added to the Phish pattern file. The Phish pattern file is a list of URLs that InterScan Web Security Virtual Appliance blocks. InterScan Web Security Virtual Appliance periodically retrieves the updated Phish pattern file through ActiveUpdate.

IWSVA allows users to submit suspected phishing URLs to TrendLabs for evaluation. TrendLabs evaluates the Web site and determines whether the submitted URL is malicious. The URL is considered malicious if it meets the criteria for one of the categories listed below.

- **Phishing:** A fraudulent collection of confidential information. This can be done by offering an email message or Web site that poses as a communication from a legitimate business, which requests information for the purpose of identity theft.
- **Spyware:** A hidden but legal program that secretly collects confidential information. Spyware monitors a user's computing habits and personal information, and then sends this information to third parties without the user's approval.

- **Virus accomplice:** An outbound HTTP request due to known behavior of malicious code—the malicious code could either send the information out or download further components from a certain URL. These are the symptoms of a spyware or Trojan infection.
- **Disease vector:** A Web site that exists only for a malicious purpose.

Blocking URLs using Phish

To block Phish categories:

1. Open the InterScan Web Security Virtual Appliance Web console and click **HTTP > URL Access Control > Global URL Blocking > Via Pattern File (Phish)**.
2. Make sure that **Enable URL blocking** is enabled.
3. Enable the phish categories to block.
4. Click **Save**.

Submitting a Suspected Phishing URL to TrendLabs

To report a suspected phishing URL to Trend Micro, use the submission form on the URL Blocking configuration screen. Submissions are investigated; and if associated with malicious behavior, the URL is added to future releases of the Phish pattern file.

1. Open the InterScan Web Security Virtual Appliance Web console and click **HTTP > URL Access Control > Global URL Blocking > Via Pattern File (Phish)**.
2. Type the URL that you want Trend Micro to investigate in the **Phish URL** field.
3. Select the **Phish categories** (either phishing, spyware, virus accomplice, disease vector, or others) that you think the URL is associated with from the menu under **Phish categories**.
4. Type an email address where you can be contacted, if necessary.
5. Add any observations about the URL that you would like to tell our TrendLabs engineers.
6. Click **Submit**.

Chapter 9

URL Filtering

This chapter presents an overview and workflow of the InterScan Web Security Virtual Appliance (IWSVA) URL filtering module with procedures for creating and configuring URL filtering policies.

URL filtering, along with Web Reputation, is part of the multi-layered, multi-threat protection solution provided by IWSVA (see Overview of URL Access Control on page 8-4).

Topics in this chapter include the following:

- Introducing URL Filtering on page 9-2
- Managing URL Filtering Policies on page 9-4
- URL Filtering Settings on page 9-8

Introducing URL Filtering

The default settings for the IWSVA URL filtering module assume that your organization's primary interest is to avoid legal liabilities associated with viewing of offensive material. However, because there are instances that require exceptions, additional policies can be created to allow access to restricted category groups for employees whose job functions require broader access. For example, members of the Human Resources or IT departments might need unrestricted Internet access to conduct investigations into violations of your organization's acceptable Internet use policies.

IWSVA supports the Safe Search feature provided by the search engine filtering providers (such as Google and Yahoo). Safe Search is used to specifically filter adult sites and content from the search results and helps protect children from exposure to adult material.

In addition, IWSVA provides enhanced filtering by combining dynamic filtering with the advanced Web Reputation databases. Browsing Web sites related to online trading, shopping, auction bidding, dating, gambling, and other non-work related activities during work time reduces employee productivity and decreases bandwidth available for legitimate browsing. IWSVA allows Internet access to be customized according to user and workgroup-specific needs, thus optimizing the use of the Internet.

IWSVA's URL filtering policies provide a granular and flexible mechanism to manage Internet access. Each policy has three basic elements that include the following:

- IWSVA access to the Web Reputation database that contains URLs in over 82 categories, such as "gambling," "games," and "personals/dating."

  Categories are contained in the following logical groups:

  - Custom Categories
  - Computers/Bandwidth
  - Computers/Harmful
  - Computers/Communication
  - Adult
  - Business
  - Social
  - General

- Access to Web sites in each category can be allowed, blocked, or monitored during time periods designated as work or leisure time.
- Different policies can be configured for different users in your environment.

Access to all identified URLs within a targeted category might be managed according to policy. The database associates each URL with one or more categories. To accurately define a Web site, the URL may belong to multiple URL categories. For example, a shopping site that contains malware may belong to the Shopping category as well as the Virus Accomplice category. Depending on how many URL categories the URL falls into, the URL filtering policy may manage the access differently. If a URL that your organization needs to access is associated with a prohibited category, you can create exceptions to URL filtering rules to override the database's classification. The patterns specified in the Approved URL List are matched against the URL, not to the content of the document to which the URL refers. IWSVA gives you the option of configuring a URL filtering approved-list by matching Web site, URL keyword, and exact-string categories.

Another way to bypass IWSVA's default URL categorization is to create Custom Categories and assign the necessary access privileges to allow user access.

The following are the filtering actions that you can apply for a given policy during the work or leisure time periods:

- **Allow**—Connection to the target server is allowed and users can access the Web site.
- **Block**—Connection to the target server is not established and users are not allowed to access the Web site. A log entry is also created for this event.
- **Monitor**—Connection to the target server is allowed and users can access the Web site. A log entry is also created for this event.
- **Warn**—Connection to the target server is allowed but a notification displays, warning users that the URL about to be accessed belongs to a category that violates company policy. Users have the option of continuing to the page or going back to the previous page.

URL Filtering Workflow

The input for URL filtering consists of the URL and the user’s ID (IP address, IP address range, user name, group name, or host name). A user is identified according to the user identification method that IWSVA is configured to use (see Configuring the User Identification Method starting on page 6-5).

A URL requested by a user can be classified into one or more of 82-plus categories, which are organized into 7 pre-defined groups. IWSVA passes the requested URL through IWSVA's URL filtering engine to be filtered according to their policies for the user making the request. Based on the category to which the requested URL belongs and the policy's action, the URL can be allowed, blocked, monitored or issued a warning.

Note: Manual updates to the URL filtering engine can be done from the **Manual Update** screen.

Managing URL Filtering Policies

IWSVA is pre-configured with two default URL filtering policies—the Global Policy that applies to all clients on the network, and the Guest Policy that applies to clients that access IWSVA through the guest port.

Note: The Guest Policy is only supported if you have configured IWSVA in stand-alone/dependent mode.

Enabling URL Filtering

Make sure that the URL filtering module is enabled before you start.

To enable URL filtering:

1. Click **HTTP > URL Filtering > Policies** from the main menu.
2. Select **Enable URL filtering**.
3. Click **Save**.

Creating a New Policy

Creating a new URL filtering policy is a four-step process:

- Select the accounts to which the policy applies.
- Specify the Web site categories to be allowed, blocked, monitored or warned during work and leisure time.
- Select the Safe Search mode
- Select an exception list

To create a new policy:

1. Open the IWSVA Web console and click **HTTP > URL Filtering > Policies** from the main menu.
2. Click **Add**.

   The **URL Filtering Policy: Add Policy** screen appears.
3. Type a descriptive **Policy name**.

   Policy names that include references to the users or groups to which they apply, for example, "URL Filtering Policy for Researchers," are easy to remember.
4. Select the users to which the policy applies.

   The options on this page depend upon the user identification method that you are using—either *IP address*, *Host name (modified HTTP headers),* or *User/group name authentication*. For more information about configuring the user identification method and defining the scope of a policy, see Configuring the User Identification Method starting on page 6-5.
5. Click **Next**.
6. On the **Specify Rules** screen, ensure that **Enable policy** is selected.
7. Select one of the following filtering actions for each URL category or sub category:
   - **Allow**—Connection to the target server is allowed and users can access the Web site.
   - **Block**—Connection to the target server is not established and users are not allowed to access the Web site. A log entry is also created for this event.
   - **Monitor**—Connection to the target server is allowed and users can access the Web site.

- **Warn**—Connection to the target server is allowed but a notification displays, warning users that the URL about to be accessed belongs to a category that violates company policy. Users have the option of continuing to the page or going back to the previous page.

8. Select to apply the filtering action during leisure or work time.
   - **Action During/Work Time**—Select the check box of the category that you want to apply the filtering action during work time. To select all the categories of a group, click the check box for the group. The group does not need to be expanded for you to select all categories in a group. Restricted days and hours are defined in the URL Filtering Settings (Schedule tab) page.
   - **Action During/Leisure Time**—Select the check box of the category that you want to apply the filtering action during leisure time. To select all the categories of a group, click the check box for the group. The group does not need to be expanded for you to select all categories in a group.
9. Click **Apply** to apply the filtering action to the selected categories.

Note: Repeat steps 8 and 9 if you want to apply a different filtering action to sub-categories in the same group.

10. Type an optional **Note** to include useful information about this policy for future reference.
11. Click **Next**.
12. Select a Safe Search setting for each search engine and click **Next**.
    - **Strict**—Filters out adult contents from all search results (including image, video, and Web search).
    - **Moderate**—Filters out adult contents from Web search results only (excluding image search).
    - **Off**—Does not filter search results. This is the default setting.
13. In the **Specify Exception Lists** screen, select an approved URL list name from the drop-down list box if you want to apply an exception list. URLs in the exception list will bypass URL filtering.
14. Click **Save**.
15. In the **URL Filtering Policies** screen, set the priority of the new policy (under the **Priority** column) by clicking on the up or down arrows.

The **Priority** setting determines which policy is applied if there are accounts belonging to two or more policies. For accounts that belong to more than one policy, IWSVA will execute the policy on a first match bases. Policies that contain the account after the first match policy is executed are skipped.

16. Click **Save**.
17. To immediately apply the policy, click **Deploy Policies Now**; otherwise, the policy is applied after the database cache expires.

Modifying and Deleting Policies

IWSVA gives you the option of editing any existing policy to better suit your current environment. You can also delete unnecessary account(s) from a policy.

To modify an existing policy:

1. Click **HTTP > URL Filtering > Policies** from the main menu.
2. Click the **Account Name** or **Policy Name** links of the policy to be modified.
3. The **URL Filtering Policy: Edit Policy** screen opens.
   - Change the scope of your policy by adding or deleting clients on the **Account** tab.
   - From the **Rule** tab, modify filtering action for the URL categories.
   - From the **Safe Search Engine** tab, change the Safe Search mode for each search engine.
   - From the **Exception** tab, select an exception list that you want to apply to this policy.
4. Click **Save**.
5. Go to **HTTP** > **URL Filtering > Policies** and set the priority of your policies using the arrows. The **Priority** setting determines which policy is applied if there are accounts belonging to two or more policies.
6. Click **Save**.
7. Click **Deploy Policies** to immediately apply the policy; otherwise, the policy is applied after the database cache expires.

URL Filtering Settings

There are several settings related to URL filtering that you can modify to reflect the realities of your work environment:

- Over 82 predefined Web site categories, organized in seven (7) logical groups
- Configuring your own custom categories
- Setting "work time" and "leisure time" schedules

Additionally, if you believe a URL is classified in the wrong category, you can send a request to Trend Micro to consider re-classifying the URL. You can also look up the category of a URL that you are not sure of.

Creating Custom Categories

You can define new URL categories in addition to the categories already provided by Trend Micro. For example, you can create a category called "Competitor's Web site" that contains the URLs of your company's competitors.

The **HTTP > Configuration > Custom Categories** screen displays a list of user-defined categories. Click **Add** to create a new one or click a category name to edit an existing one.

- **Category Name**—Type a brief but descriptive name for the custom category. Names must be unique.
- **Match**—Enter a Web site, a keyword or phrase, or a string of characters in the field, and then tell IWSVA how to apply the match. This field supports both the ? and * wildcards. Entries in this field are added one-by-one to the custom category.

Note: For HTTPS decryption policies, the strings to match vary depending on whether you set IWSVA in proxy or transparency mode.
- In proxy mode, IWSVA matches the domain names, not the full URL. Thus, you only need to specify the domain names.
- In transparency mode (WCCP and Bridge mode), IWSVA matches the CommonNames in the server certificates received.

  - **Web site**—Limits the search to the string as a whole; used with one or more wildcards, this type of setting can be especially useful for applying the configured URL filtering action to an entire Web site. There is no need to include http:// or https:// in the URL (it is automatically stripped).
  - **URL keyword**—Looks for any occurrence of the letters and/or numbers within a URL, and will match regardless of where the string is found (the string "sex" would be considered a match for "http://www.encyclopedia/content/sexton.htm" and the page blocked). Using wildcards in this field greatly increases the chance of false positives and unexpected results.
  - **String**—Limits the search to the string as a whole, for example to target a specific site, page, file, or other particular item.
- **Import URL List**—You can import an existing list of URLs that you want to add to a category. For example if you have a list of your competitors' URLs you have compiled using a text editor, you can import the list rather than enter them one-by-one. Import lists must conform to a defined standard (refer to the online help for more information).

Requesting URL Reclassification and URL Lookup

Organized in seven logical groups, IWSVA includes default categories that provide a baseline level of URL filtering. For example, Web sites related to humor and jokes would be found in the "Joke Programs" category, which is located in the *Computers/Bandwidth* group.

If you do not agree with the default classification of a URL, Trend Micro enables you submit a request for a reclassification. You can also use the Exception List or Custom Categories to bypass domain and Web site ratings categorized by Trend Micro's URL filtering database.

Before rolling out URL filtering policies, Trend Micro recommends verifying that the default categorizations are appropriate for your organization. For example, a clothing retailer might need to remove a swimsuit Web site from the "Intimate Apparel/Swimsuit" category located in the *Adult* group in order to allow legitimate market and competitor research.

If you want to know a category of a URL, you can look it up when specifying URL filtering settings in the **HTTP > URL Filtering > Settings > URL Filtering > Settings** screen (**URL Re-classification & Lookup** tab).

Unrated and Unknown URLs

An *unrated* URL is a Web site that Trend Micro knows about but has not yet put into a filtering category.

An *unknown* URL is a Web site that is one of the following:

- Unknown to Trend Micro
- A Web site that is not in the Web Reputation database
- The daemon might be down or the remote rating server is inaccessible to give the URL a rating

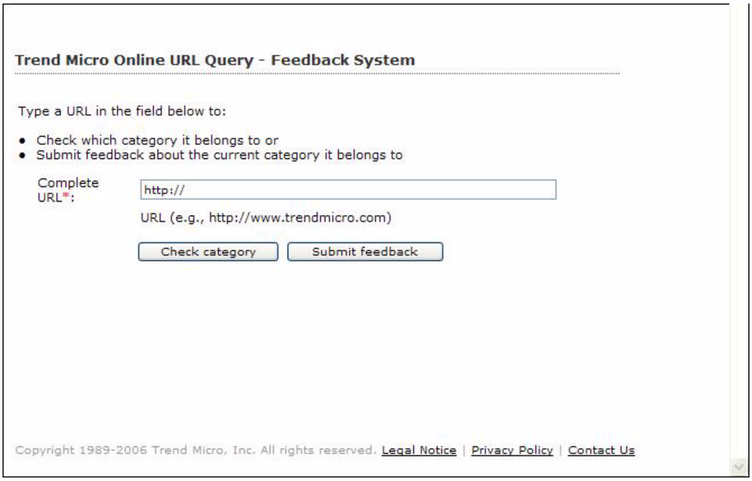
An unknown URL has a rating of zero (0) and cannot be blocked.

Requesting a Reclassification

To request a URL reclassification:

1. Click **HTTP > URL Filtering > Settings** from the main menu.
2. Click the **URL Re-classification & Lookup** tab.
3. Click on the URL.

   The Trend Micro Online URL Query - Feedback System screen appears.



Trend Micro Online URL Query - Feedback System

Type a URL in the field below to:

- Check which category it belongs to or
- Submit feedback about the current category it belongs to

Complete URL*: http://

URL (e.g., http://www.trendmicro.com)

Check category
Submit feedback
Copyright 1989-2006 Trend Micro, Inc. All rights reserved. Legal Notice | Privacy Policy | Contact Us

FIGURE 9-1. Trend Micro Online URL Query - Feedback System screen

4. Complete all the necessary information and click **Submit Feedback**.

Work and Leisure Schedule Settings

IWSVA enables you to specify two sets of work times: Work Time 1 and Work Time 2. Both of these work times include 24-hour selections.

When creating URL filtering policies, you can set the policy to be in effect for both Work Time 1 and Work Time 2 and/or during “leisure” time. When you set a policy for Work Time 1, it is also in effect for Work Time 2.

IWSVA policies permit or block access to URL categories during work and leisure time. By default, IWSVA uses the following default work time settings:

- Work days: Monday to Friday
- Work hours: 8:00 to 11:59 (Work Time 1) and 13:00 to 17:00 (Work Time 2).

Time not defined as work hours is considered “leisure” time.

Note: It is assumed that all IWSVA devices in a cluster are within the same time zone.

Before implementing URL filtering policies in your organization, Trend Micro recommends verifying that the work and leisure time settings are appropriate for your environment.

To configure the URL filtering policy schedule:

1. Open the IWSVA Web console and click **HTTP > URL Filtering > Settings > Schedule**.
2. Under **Work Time Settings**, select the work days and work hours in the fields provided.

   In the Work Time 1 and/or Work Time 2 areas, specify the hours that you want to restrict access to selected URL categories.
3. Click **Save**.

To specify no work time or all work time:

- If you do not want to use work times, uncheck all of the work days. All time is then leisure time.
- If you want all time to be work time, select all days and specify the following:
  - For Work time 1, choose "0:00" in the **From** drop-down list and "11:59" in the **To** drop-down list.
  - For Work time 2, choose "12:00" in the **From** drop-down list and "23:59" in the **To** drop-down list.

URL Access Warning TTL

The URL Access Warning Time-to-Live (TTL) setting allows the administrator to configure the amount of time between displayed warning messages, if the user chooses to be reminded after the initial warning messages displays.

Note: The repeated warning message only occurs if the user opts to continue to a Web page after the initial warning message.

The default value is 5 minutes. This setting is configured per user/per category.

The warning message displays if the value for the policy rule's selected action is set to Warn. See Creating a New Policy on page 9-5 for more information.

See Configuring URL Access Warning Notifications on page 12-53 for more about the notifications.

URL Filtering Exceptions

IWSVA provides the option to configure exceptions to URL filtering by approved lists (see Specifying the Exception Lists on page 7-38). URLs in the exception list will not be blocked or monitored. If your clients have a legitimate need to view Web sites that are being blocked or monitored by URL filtering, include the URL to an approved URL list and apply the list to the policy.

Note: IWSVA still applies Safe Search filtering to Web sites in the approved URL list.

To apply an approved URL list to a URL filtering policy:

1. Open the IWSVA Web console and click **HTTP > URL Filtering > Policies** and click a policy name to edit it.
2. In the **Exceptions** tab, select the approved URL list name.

   Note: URLs in the exception list will not be warned. For more information, see Configuring URL Access Warning Notifications on page 12-53.

3. Click **Save**.

Chapter 10

FTP Scanning

This chapter describes FTP virus scanning and the different ways FTP scanning can be deployed and configured for your environment.

Topics in this chapter include:

Introduction

InterScan Web Security Virtual Appliance (IWSVA) can scan FTP uploads and downloads for viruses and other malicious code in a manner similar to how it processes HTTP traffic. Unlike HTTP scanning, however, a single configuration is applied to all clients on your network—user or group-based policies are not supported for FTP scanning.

IWSVA FTP scanning uses either a stand-alone proxy or works in conjunction with another FTP proxy on the network. To deploy FTP scanning into your environment, first configure the FTP settings that control the type of proxy and the type of data connection (either passive or active FTP; see Passive and Active FTP starting on page 10-3). The next step is to configure the scanning rules that control the traffic direction that is scanned, the type of files to block or scan, how compressed and large files are handled, and the actions taken when malicious code is detected.

After setting the FTP scanning settings, there are optional security and performance settings to consider modifying. Access control lists can be configured to selectively allow client FTP access based on the client's IP address. To improve performance when frequently accessing FTP sites over which you have direct control of the content, specific FTP servers can be added to an approved list so that downloads from them are not scanned. Moreover, to further lock down the IWSVA device, FTP access to specific ports can either be allowed or denied.

Note: IWSVA does not support active FTP scanning in WCCP mode.

FTP Settings

IWSVA FTP scanning settings include options for using either the IWSVA native (stand-alone) proxy or a separate FTP proxy, two options for how data connections are made (active FTP vs. passive FTP).

Proxy Settings

IWSVA FTP scanning provides two proxy options—a "stand-alone" mode whereby clients connect to the native IWSVA proxy that later connects with the FTP server, and an "FTP proxy" mode whereby IWSVA passes requests through a separate FTP proxy that in turn connects to the FTP server.

- In stand-alone mode, the client needs to use `<username>@<FTP server name>` as the FTP username to indicate which FTP server IWSVA should connect to.
- In FTP proxy mode, no username is required because IWSVA always connects to the FTP proxy and server designated in the configuration settings.

FTP proxy mode can also be used to protect a single FTP server by specifying the FTP server's hostname/IP address and port number in the FTP proxy configuration. In this case, the IWSVA FTP scanning module is dedicated to the specified FTP server, in a manner similar to a reverse proxy for HTTP scanning.

Passive and Active FTP

IWSVA uses either active or passive FTP for data connections, depending on your firewall setting. FTP uses two ports, a data port and a command port. In *active* FTP, the server connects to the client to establish the data connection. In *passive* FTP, the client connects to the server.

When passive FTP is selected in the IWSVA configuration, IWSVA converts the "active" mode on the client side into the "passive" mode on the server side. Mode conversion is performed only when the IWSVA configuration is passive and the client uses the active mode. If the IWSVA configuration is active, no conversion is performed, so passive requests from the client are still passive requests on the server side.

Client Requests

To configure the FTP settings, you need to specify the proxy settings and the data connection.

To configure the FTP settings:

1. Click **FTP > Configuration > General** from the main menu.
2. Under the **Proxy Settings** section, select the appropriate FTP setting based on your topology—either **Use stand-alone mode** if you want the native IWSVA proxy to connect to FTP sites, or **Use FTP proxy** for the FTP service to work with an existing FTP proxy (specify the host name of the **Proxy server** and the **Port**).
3. Choose the type of data connection to use—either **Passive FTP** or **Active FTP**.
4. Click **Save**.

FTP Scanning Options

The FTP virus scanning settings are similar to the HTTP scanning settings, with two differences:

- FTP scanning does not support user or group-based policies; therefore, one configuration is applied to all clients that access the FTP sites through IWSVA.
- The traffic direction to scan can be configured—either to uploads, downloads, or both.

Enabling FTP Traffic and FTP Scanning

Before your clients can access the FTP sites through IWSVA, the FTP traffic must be enabled.

To turn on the FTP traffic:

1. Click **Summary** in the main menu.
2. Click **Turn On** or **Turn Off** (at the top of the screen) to start or stop the FTP traffic flow.

   Turn Off means the FTP service on the IWSVA device is shut down; therefore, clients cannot connect to any FTP servers through the IWSVA FTP proxy. The default setting is **On**.

   After the FTP traffic is enabled, FTP scanning must be turned on.

To enable or disable FTP scanning:

1. Open the IWSVA Web console and click **FTP > Scan Rules**.
2. Select **Enable FTP scanning**.
3. Click **Save**.

Scan Direction

Depending on how you want to use IWSVA FTP scanning, you can selectively configure the FTP scanning module to scan uploads, downloads or both. For example, if you have deployed antivirus software to all of the workstations in your organization, disabling uploads might be justified to achieve a performance benefit, because the files should already be scanned on the client.

File Blocking

You can specify the types of files to block for security, monitoring or performance purposes. You can block file types such as Java applets, Microsoft Office documents, audio/video files, executables, images, or other types that you can manually configure. If your organization has policies that prohibit certain types of files in your network, IWSVA FTP file blocking can stop them at the FTP gateway.

File Scanning

When configuring the types of files to be scanned, there are three options:

- **All scannable files:** All files are scanned (the safest option).
- **IntelliScan:** Only file types known to harbor viruses are scanned (file type is determined by checking the file header). See About IntelliScan starting on page 7-24 for more information.
- **Specified file extensions:** Only files with specified file extensions are scanned.

Trend Micro recommends scanning all files, unless performance considerations require choosing one of the other options. See *Configuring FTP Scanning Settings* on page 10-7 for more information.

Priority for FTP Scan Configuration

If the configurations on the **FTP Virus Scan** screen conflict with each other, the program scans according to the following priority:

1. Block these file types
2. Scan these file types (if not blocked)

Compressed File Handling

Compressed files can pose special challenges to antivirus software performance, because they must be decompressed before the individual files within the archive can be scanned. IWSVA provides the option to block, quarantine, or pass all compressed files at the gateway.

Alternatively, you can also configure IWSVA to apply the selected action on compressed files that meet one of the following conditions:

- Decompressed file count exceeds a given threshold
- Cumulative decompressed file size exceeds a configured maximum
- Recursively compressed file exceeds a certain number of compressed layers

Note: IWSVA can also block specified file types within a compressed file during FTP scanning.

Large File Handling

If the delay when downloading large files is unacceptable, IWSVA can be configured to skip scanning of files larger than a configured threshold. Additionally, the FTP scanning module can use the "deferred scanning" method for large files to prevent the client connection from timing out. See Deferred Scanning starting on page 7-31 for more information.

Note: The FTP scanning module does not support the "scan before delivering" large file handling methods used by the HTTP scanning module.

Encrypting Quarantined Files

If IWSVA is configured to quarantine files as a scan action, it can optionally encrypt the files to prevent them from accidentally being executed by someone browsing the quarantine folder. Note that after encrypted, the files can only be decrypted by a representative from Trend Micro's Support department.

Scanning for Spyware/Grayware

IWSVA can scan for many additional non-virus risks for which patterns are contained in the spyware/grayware pattern file. For a summary of these risks, see Spyware and Grayware Scanning Rules starting on page 7-34.

FTP Scanning Exception List

You can apply an approved list that contains the names of files that you want to exempt from file type blocking. In addition, you can configure IWSVA to bypass virus/spyware scanning and compressed file handling action on files in an approved list.

For more information, see Specifying the Exception Lists on page 7-38.

Configuring FTP Scanning Settings

To configure FTP scanning:

1. Click **FTP > Scan Rules** from the main menu.
2. Select **Enable FTP scanning**.
3. Select the types of FTP transfers to scan—either **Upload**, **Download**, or both.
4. Under the **Block these file types** section, select the file types to be blocked. In the **Other file types** field, type other file types to block (use a space to delimit multiple entries). See Appendix B, *Mapping File Types to MIME Content-types* for a list of other file types that can be blocked.

5. Select the files to scan:
   - To scan all file types regardless of extension, select **All scannable files**. IWSVA opens compressed files and scans all files within. Scanning all files is the most secure configuration.
   - To use true-file type identification, select **IntelliScan**. IntelliScan uses a combination of true attachment type scanning and exact extension name scanning. True attachment type scanning recognizes the file type even when the file extension has been changed. IntelliScan automatically determines which scanning method to use.
   - To scan file types based on their extensions, select **Specified file extensions**. This contains the list of file types known to harbor viruses. IWSVA scans only those file types that are explicitly specified in the **Default Extensions** list and in the **Additional Extensions** text box. The default list of extensions is periodically updated from the virus pattern file.

     Use this option, for example, to decrease the aggregate number of files IWSVA checks, therefore, decreasing the overall scan times.

Note: There is no limit to the number or types of files you can specify. Do not precede an extension with the (*) character. Delimit multiple entries with a semicolon.

6. Under **Compressed file handling**, select an action (Block, Quarantine, or Pass) and select to apply the action to one of the following:
   - All compressed files
   - Compressed files if

   If you enable the second option, type a value for the following parameters:
   - Decompressed file count exceeds (default is 50000)
   - Size of a decompressed file exceeds (default is 200MB)
   - Number of layers of compression exceeds (0-20, default is 10)
   - Compression ratio of any file in the archive exceeds 99 percent
7. Under **Large File Handling**, select **Do not scan files larger than** and enter the file size.
8. To avoid browser time-out issues when downloading large files, select **Enable Deferred Scan** and type the file size above which deferred scanning occurs. Also,

select from the drop-down list the percentage of data to be sent to the client unscanned.

WARNING! **The partial delivery of a file might result in a virus leak; therefore, this would be a performance versus an absolute security choice for you. Use this option only when you are currently experiencing an issue with timeouts.**

9. To encrypt files sent to the quarantine directory to prevent them from being inadvertently opened or executed, select **Encrypt quarantined files**.
10. Click **Save** and switch to the **Spyware/Grayware Scan Rule** tab.
11. Select the types of additional risks to scan for, and click **Save**.
12. In the **Exceptions** tab, select an approved file name list from the drop-down list.

    Select **Do not scan the contents of selected approved lists** if you do not want to scan the contents of the files in the approved lists for viruses. In addition, compressed file handling action will not be applied.
13. Switch to the **Action** tab, and select the actions for IWSVA to take in response to scanning.
14. Click **Save**.

Setting Scan Actions on Viruses

You can specify the action for FTP scanning to take upon finding an infected file (the recommended action setting is **Clean**):

- Choose **Quarantine** to move an infected file to the quarantine directory without cleaning. The requesting client does not receive the file.
- Choose **Delete** to delete an infected file at the server. The requesting client does not receive the file.
- Choose **Clean** to automatically clean and process an infected file. The requesting client receives the cleaned file if it is cleanable.

You can specify the action for FTP scanning to take upon finding an uncleanable file, which includes worms and Trojans (the recommended action setting is **Delete**):

- Choose **Pass** to send an uncleanable file to the client without cleaning (Trend Micro does not recommend this choice, because it might allow infected files into your network).
- Choose **Quarantine** to move, without cleaning, an uncleanable file to the quarantine directory. The requesting client does not receive the file.
- Choose **Delete** to delete an uncleanable file at the server. The requesting client does not receive the file.

You can specify the action for FTP scanning to take in handling a password-protected compressed file (the recommended action setting is **Pass**):

- Choose **Pass** to send a password-protected file to the client without cleaning.
- Choose **Quarantine** to move, without cleaning, a password-protected file to the quarantine directory. The requesting client does not receive the file.
- Choose **Delete** to delete a password-protected file at the server. The requesting client does not receive the file.

In the event a file containing macros (not necessarily macro viruses) is detected during FTP transfers, the following actions are available (the recommended action setting is **Pass**).

- Choose **Quarantine** to move the files containing macro(s) to the quarantine directory.
- Choose **Clean** to remove macros before delivering the file.
- Choose **Pass** to disable special handling of files containing macro(s).

FTP Access Control Settings

IWSVA includes several access control settings for additional security and performance tuning:

- FTP access can be enabled based on the client's IP address.
- Trusted servers over which you have close control of their content and are frequently accessed can be added to an approved list and transfers are not scanned for a performance benefit.
- The IWSVA FTP server can be locked down by denying access to ports that you configure.

By Client IP

By default, all clients on the network are allowed to access FTP sites through the IWSVA device (provided FTP traffic is enabled, see Enabling FTP Traffic and FTP Scanning starting on page 10-4).

To limit FTP access based on client IP address:

1. Click **FTP > Configuration > FTP Access Control** from the main menu.
2. Switch to the **Client IP** tab.
3. Select **Enable FTP Access Based on Client IP**.
4. Enter the IP addresses of clients allowed FTP access through IWSVA. The following are acceptable entries:
   - **IP**: a single IP address, for example, 123.123.123.12.
   - **IP Range**: clients that fall within a contiguous range of IP addresses, for example, from 123.123.123.12 to 123.123.123.15.
   - **IP Mask**: a single client within a specified subnet, for example, entering IP = 192.168.0.1 and Mask = 255.255.255.0 identifies all machines in the 192.168.0.x subnet. Alternatively, the Mask can be specified as a number of bits (0 to 32).
5. Type a descriptive name in the **Description** field. (40 characters maximum)
6. Click **Add** and continue entering other clients that are allowed to access FTP sites.
7. Click **Save**.

Via Approved Server IP List

To reduce possible performance issues when accessing trusted FTP sites over which you directly control the content, you can exempt some FTP sites from scanning by adding their IP addresses to an approved list.

Note: Skipping scanning through the IP approved list only applies to file downloads. Uploaded files are still scanned.

To add trusted servers to the approved list:

1. Click **FTP > Configuration > FTP Access Control** from the main menu.
2. Switch to the **Approved Server IP List** tab.

3. Enter the IP addresses of FTP sites to exempt from IWSVA FTP virus scanning. See Identifying Clients and Servers starting on page 5-13 for information and examples about how to identify the servers.
4. Type a descriptive name in the **Description** field. (40 characters maximum)
5. Click **Add** and continue entering other FTP sites to exempt.
6. Click **Save**.

Via Destination Ports

By default, clients can access any port on the IWSVA FTP server. To increase security, you can selectively allow or deny access to the ports.

To configure IWSVA FTP ports to which clients can connect:

1. Click **FTP > Configuration > FTP Access Control** from the main menu.
2. Switch to the **Destination Ports** tab.
3. Choose the action to apply to a port, either **Deny** or **Allow**.
4. Enter the **Port** or **Port Range** to which the action applies.
5. Type a descriptive name in the **Description** field. (40 characters maximum.)
6. Click **Add**.
7. Continue to add other ports to allow or deny.
8. Click **Save**.

Note: The destination port list at the bottom of the **Destination Port** tab reflects the processing order (or reverse priority order). Destination port access control is only applied during an FTP command connection, and FTP data connections are not affected. A typical configuration is 1. "Deny ALL" and 2. "Allow 21" which results in only allowing access to port 21.

Chapter 11

Command Line Interface Commands

This chapter describes the Command Line Interface (CLI) commands that you can use in the InterScan Web Security Virtual Appliance (IWSVA) product to perform monitoring, debugging, troubleshooting, and configuration tasks.

CLI commands allow administrators to perform additional configuration tasks, such as enabling and disabling Squid caching, and to perform debug and troubleshooting functions. The CLI interface also provides additional commands to monitor critical resources and functions, such as monitoring the traffic that flows in or out of a network interface.

Topics included in this chapter are:

- SSH Access starting on page 11-2
- Command Modes starting on page 11-3
- Command List starting on page 11-3

SSH Access

Access to the IWSVA CLI interface can be obtained through the IWSVA terminal (keyboard and monitor connected directly to the IWSVA server) or remotely using a SSH v2 connection to the management IP address. Before you access the CLI using SSH, you must first enable SSH access control in the Web console (**Administration > Network Configuration > Remote CLI**).

Preventing Password Brute Force Attacks through SSH

IWSVA can protect against password brute force attacks. If a remote terminal attempts to log on to IWSVA with the wrong password using SSH, IWSVA will reject subsequent log on attempts. This feature is enabled and disabled through the CLI.

To enable the anti-password brute force attack function:

1. Log on to IWSVA using the root, enable, or admin account. "root" and "admin" account users can log on using SSH, but the "enable" account users can only log on to the IWSVA local machine.

- If logging on with the root account, type **`clish`** and **`enable`** to access the clish privileged mode.
- If logging on with the admin account, type **`enable`** to access the clish privileged mode.
- If logging on with the enable account, you are already in the clish privileged mode.

2. To enable the function, type the following command: **`configure service pswd_protection enable`**

To disable the anti-password, brute force attack function:

1. Follow Step 1 in the previous procedure.

2. To disable the function, type the following command: **`configure service pswd_protection disable`**.

Command Modes

To access the CLI interface, you will need to have the administrator account and password. IWSVA's CLI commands are separated into two categories—non-privileged and privileged commands.

Non-privileged commands are basic commands that allow the administrator to obtain specific low security risk information and to perform simple tasks. The non-privileged command prompt ends with an angle bracket (>).

Privileged commands provide full configuration control and advanced monitoring and debugging features. To use privileged commands, type `enable` and the password for the Enable account. The screen displays `enable#` as the privileged command prompt. To return to non-privileged commands, type `exit`.

Note: Some CLI commands are not available to child members of an HA cluster. because these parameters need to be configured through the parent member of the cluster. Some of the commands unavailable through the child server are: `configure system date`, `configure module ntp`, `configure system password`, `configure service ssh`, and `configure system timezone`

Command List

Note: Commands have been standardized. Commands with syntax changes from a previous release show the new command syntax first, followed by the replaced command syntax. For example:

```
start shell
```

Replaces:

```
admin shell
```

The following table lists the available commands:

TABLE 11-1. Command Line Interface Commands

COMMAND	SYNTAX	DESCRIPTION
configure module arm disable **Replaces:** disable ARM	configure module arm disable	Force un-registration to ARM
configure module database password **Replaces:** configure db password	configure module database password	Configure the database password
configure module http bypass_non_http disable **Replaces:** disable bypass_non_http	configure module http bypass_non_http disable	Disable non-HTTP traffic bypass
configure module http bypass_non_http enable **Replaces:** enable bypass_non_http	configure module http bypass_non_http enable	Enable non-HTTP traffic bypass
configure module http scan_before_deliver_port **Note:** This is a new command.	configure module http scan_before_deliver_port <port> [mgmt_interface]	Configure the redirecting port to scan before delivery

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module http x-forwarded-for action add **Note:** This is a new command.	configure module http x-forwarded-for action add	Add the IP address of the last hop to the XFF HTTP header
configure module http x-forwarded-for action keep **Note:** This is a new command.	configure module http x-forwarded-for action keep	Make no changes in the XFF HTTP header
configure module http x-forwarded-for action remove **Note:** This is a new command.	configure module http x-forwarded-for action remove	Remove the XFF HTTP header from the HTTP request for upstream security
configure module http x-forwarded-for parse disable **Note:** This is a new command.	configure module http x-forwarded-for parse disable	Disable parsing of the XFF HTTP header
configure module http x-forwarded-for parse enable **Note:** This is a new command.	configure module http x-forwarded-for parse enable	Enable parsing of the XFF HTTP header to obtain the original IP address for policy matching
configure module https hardware_engine cavium	configure module https hardware_engine cavium	Use “cavium” hardware accelerate card; this operation requires that the hardware card be inserted into the machine

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module https hardware_engine none	configure module https hardware_engine none	Do not use SSL hardware accelerate card
configure module https iis_client_certificate <enable/disable> **Replaces**: <disable/enable> iis_client_certificate	configure module https iis_client_certificate <enable/disable>	Configure iis_client_certificate
configure module https iis_client_certificate_ sites clear **Replaces:** clear iis_client_certificate_ sites	configure module https iis_client_certificate_ sites clear	Clear the cache of IIS hosted HTTPS sites with client certificate required
configure module https logacccfullurl **Replaces:** <disable | enable> https logaccfullurl	configure module https logacccfullurl <enable/disable>	Configure logaccfullurl

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module identification mac_address <enable/disable> **Replaces:** configure mac address no configure mac address yes	configure module identification mac_address <enable/disable>	Include/exclude MAC address for hostname identification method
configure module ldap groupcache interval **Replaces:** configure ldap groupcache interval <interval>	configure module ldap groupcache interval <interval>	Configure IWSVA LDAP user group membership cache interval *interval* UINT interval (in hours)
configure module ldap ipuser_cache disable **Replaces:** configure ldap ipuser_cache disable	configure module ldap ipuser_cache disable	Disable IWSVA LDAP IP user cache
configure module ldap ipuser_cache enable **Replaces:** configure ldap ipuser_cache enable	configure module ldap ipuser_cache enable	Enable IWSVA LDAP IP user cache

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module ldap ipuser_cache interval **Replaces:** configure ldap ipuser_cache interval <interval>	configure module ldap ipuser_cache interval <interval>	Configure IWSVA LDAP IP user cache interval *interval* FLOAT interval (in hours)
configure module ldap www-auth port **Replaces:** configure www-auth port <port>	configure module ldap www-auth port <port>	Configure the user/group authentication port in transparent mode (WCCP or bridge mode)
configure module log transaction disable **Note:** This is a new command.	configure module log transaction disable	Disable the Transaction Log
configure module log transaction enable **Note:** This is a new command.	configure module log transaction enable	Enable the Transaction Log
configure module log transaction filter disable **Note:** This is a new command.	configure module log transaction filter disable	Disable the Transaction Log filter.

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module log transaction filter enable **Note:** This is a new command.	configure module log transaction filter enable <fromip> <toip>	Enable the Transaction Log filter. PARAM name: "fromip" IP address AAA.BBB.CCC.DDD where each part is in the range 0-255 PARAM name: "toip" IP address AAA.BBB.CCC.DDD where each part is in the range 0-255
configure module log verbose filter disable **Note:** This is a new command.	configure module log verbose filter disable	Disable verbose log filter
configure module log verbose filter enable fromip toip **Note:** This is a new command.	configure module log verbose filter enable fromip toip	Enable verbose log filter
configure module log verbose ftp disable **Replaces:** disable verbose ftp	configure module log verbose ftp disable	Disable verbose FTP logs

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module log verbose ftp enable **Replaces:** enable verbose ftp	configure module log verbose ftp enable	Enable verbose FTP logs
configure module log verbose http disable **Replaces:** disable verbose http	configure module log verbose http disable	Disable verbose HTTP logs
configure module log verbose http enable **Replaces:** enable verbose http	configure module log verbose http enable	Enable verbose HTTP logs
configure module log verbose wccp disable **Replaces:** disable verbose wccp	configure module log verbose wccp disable	Disable verbose WCCP logs
configure module log verbose wccp enable **Replaces:** enable verbose wccp	configure module log verbose wccp enable	Enable verbose WCCP logs
configure module ntp schedule <enable/disable> **Replaces:** disable ntp schedule enable ntp schedule	configure module ntp schedule <enable/disable>	Enable or disable scheduled NTP time synchronization

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure module ntp schedule **Replaces:** configure ntp schedule <interval> <primary_server> [secondary_server]	configure module ntp schedule <interval> <primary_server> [secondary_server]	Configure scheduled NTP time synchronization *interval* (30m, 1h, 2h, 4h, 6h, 12h, 1d, 2d, 3d, 1w, 1M) *primary_server* ADDRESS Primary NTP server *secondary_server* ADDRESS Secondary NTP server
configure module ntp sync **Replaces:** configure ntp sync <server>	configure module ntp sync <server>	Configure NTP server synchronization *server* ADDRESS NTP server
configure network bonding add	configure network bonding add <bondingname> [interface1] [interface2] [interface3] [interface4]	Add a link aggregation bonding interface <bondingname> is the name of the bonding interface
configure network bonding options miimon	configure network bonding options miimon <interval>	Configure miimon options of specified bonding device <interval> is the specific miimon interval to be set. Default is 100. **Note:** Miimon is a value setup in milli-seconds.

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure network bonding options xmit_hash_policy	configure network bonding options xmit_hash_policy <policy>	Configure xmit_hash_policy options of specified bonding device <policy> is the specific xmit_hash_policy to be set Default is 1 (3layer). 0 (2layer) is also available.
configure network bonding remove	configure network bonding remove <bondingname>	Remove a link aggregation bonding interface <bondingname> is the name of the bonding interface
configure network bridge interface **Replaces:** configure bridge interface <internal> <external>	configure network bridge interface [interface1] [interface2] [interface3] [interface4] [interface5] [interface6] [interface7] [interface8]	Configure the default bridge interface *internal* IFNAME Interface name or link aggregation bonding name *external* IFNAME Interface name or link aggregation bonding name
configure network bridge redirect ftpports **Replaces:** configure redirect ftpports <ports>	configure network bridge redirect ftpports <ports>	Configure the redirection ftp ports *ports* MULTIPORTS Redirect ports <port1;port2;...>

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure network bridge redirect httpports **Replaces:** configure redirect ftpports <ports>	configure network bridge redirect httpports <ports>	Configure the redirection HTTP ports *ports* MULTIPORTS Redirect ports <port1;port2;...>
configure network bridge redirect httpsports Replaces: configure redirect httpsports <ports>	configure network bridge redirect httpsports <ports>	Configure the redirection HTTPS ports *ports* MULTIPORTS Redirect ports <port1;port2;...>
configure network bridge stp **Note:** This is a new command.	configure network bridge stp	Configure the default bridge STP settings
configure network bridge stp disable **Note:** This is a new command.	configure network bridge stp disable	Disable STP on IWSVA
configure network bridge stp enable **Note:** This is a new command.	configure network bridge stp enable	Enable STP on IWSVA
configure network bridge stp priority **Note:** This is a new command.	configure network bridge stp priority	Set the STP priority of IWSVA

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure network dns **Replaces:** configure dns	configure network dns <dns1> [dns2]	Configure DNS settings *dns1* IP_ADDR Primary DNS server *dns2* IP_ADDR Secondary DNS server
configure network hostname **Replaces:** configure hostname	configure network hostname <hostname>	Configure the hostname hostname HOSTNAME Hostname or FQDN
configure network interface dhcp <interface_name> [vlan] **Replaces:** configure mgmt ip static <ip> <mask> **Note:** The old command does not map directly to the new command. Changes were made to support the updated release.	configure network interface dhcp <interface_name> [vlan]	Configure the default Ethernet interface to use DHCP vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure network interface duplex **Replaces:** configure ethernet duplex <ethname> <duplex>	configure network interface duplex <ethname> <duplex>	Configure the duplex of the Ethernet interface

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure network interface ping <interface_name> <action> **Replaces:** enable/disable ping [mgmt]	configure network interface ping <interface_name> <enable/disable>	Accept/disallow ICMP-request on the separated management interface
configure network interface static **Replaces:** configure ip static <ip> <mask> <gateway> [vlan]	configure network interface static <interface_name> <ip> <mask> [vlan]	Configure the default Ethernet interface to use the static IP configuration
configure network lanbypass auto	configure network lanbypass auto	The system auto-adjusts the LAN bypass status.
configure network lanbypass off	configure network lanbypass off	Never bypass traffic
configure network lanbypass on	configure network lanbypass on	Always bypasses traffic
configure network mgmt disable	configure network mgmt disable	Disable the separate IWSVA management interface
configure network mgmt interface **Replaces:** configure mgmt interface <interface_name>	configure network mgmt interface <interface_name>	Configure IWSVA management interface name

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure network portgroup add **Note:** This is a new command.	configure network portgroup add <pgname> [interface1] [interface2] [interface3] [interface4] [interface5] [interface6] [interface7] [interface8]	Add a port group
configure network portgroup linkloss <pgname> **Note:** This is a new command.	configure network portgroup linkloss <pgname>	Configure the port group link loss forward settings
configure network portgroup remove <pgname> **Note:** This is a new command.	configure network portgroup remove <pgname>	Remove a port group
configure network portgroup vlan <pgname> **Note:** This is a new command.	configure network portgroup vlan <pgname>	Configure the port group VLAN ID
configure network proxy interface **Replaces:** configure proxy interface <proxy>	configure network proxy interface <proxy>	Configure the default proxy interface *proxy* IFNAME Interface name

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure network route add <ip_prefixlen> <via> <dev> **Note:** This is a new command.	configure network route add <xxx.xxx.xxx.xxx/LL> <via> <device>	Add a route for a specified NIC device in VA
configure network route default <gateway> **Replaces:** configure ip dhcp [vlan] **Note:** The old command does not map directly to the new command. Changes were made to support the updated release.	configure network route default <gateway>	Reset the default gateway by executing configure network route default <*.*.*.*>
configure network route del <ip_prefixlen> <via> <dev> **Note:** This is a new command.	configure network route del <xxx.xxx.xxx.xxx/LL> <via> <device>	Delete a route for a specified NIC device in VA
configure service pswd_protection disable **Note:** This is a new command.	configure service pswd_protection disable	Disable SSH password protection service

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure service pswd_protection enable **Note:** This is a new command.	configure service pswd_protection enable	Enable SSH password protection service
configure service recycle time **Note:** This is a new command.	configure service recycle time	Enable recycling by time PARAM name "time" Use hh:mm time format between 00:00 and 23:59
configure service recycle disable time **Note:** This is a new command.	configure service recycle disable time	Disable recycling by time
configure service recycle transaction **Note:** This is a new command.	configure service recycle transaction	Enable recycling by transaction PARAM name "transaction" Daemon will recycle after 100000-99999999 transaction(s)
configure service recycle disable transaction **Note:** This is a new command.	configure service recycle disable transaction	Disable the transaction recycling
configure service ssh disable **Replaces:** disable ssh	configure service ssh disable	Disable the SSH daemon

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure service ssh enable **Replaces:** enable ssh	configure service ssh enable	Enable the SSH daemon
configure service ssh port **Replaces:** configure ssh port <port>	configure service ssh port <port>	Configure SSH port number *port* PORT SSH port number [1 ~ 65535]
configure system date **Replaces:** configure date	configure system date <date> <time>	Configure date and save to CMOS *date* DATE_FIELD [DATE_FIELD] *time* TIME_FIELD [TIME_FIELD]
configure system ha **Note:** This is a new command.	configure system ha	Configure high availability
configure system ha remove **Note:** This is a new command.	configure system ha remove	Remove HA configuration and reboot IWSVA
configure system ha synchronization interval **Note:** This is a new command.	configure system ha synchronization interval	Configure the HA synchronization interval PARAM name: "Interval" Interval (in minutes) at which HA will synchronize settings to child server. Range in minutes: 5-60

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system harddisk	configure system harddisk	Add new hard disk and extend IWSVA data partition space **Note:** IWSVA only supports adding one new hard disk and extends the IWSVA data partition space each time.
configure system hwmonitor **Note:** This is a new command.	configure system hwmonitor	Configure system hardware monitoring information.
configure system hwmonitor interval **Note:** This is a new command.	configure system hwmonitor interval [1-60]	Configure hardware status polling in minutes. Range is 1-60 minutes. Default duration determined by the IPMI polling cycle.
configure system keyboard	configure system keyboard	Configure system keyboard layout type
configure system keyboard us	configure system keyboard us	Configure system keyboard layout type to U.S. English

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system password **Replaces:** configure password	configure system password <user>	Configure account password *user* USER The user name for which you want to change the password. The user could be 'enable', 'root' or any user in the IWSVA's Administrator group
Note: All “configure system timezone” commands replace the old “configure timezone” commands.		
configure system timezone Africa Cairo	configure system timezone Africa Cairo	Configure timezone to Africa/Cairo location
configure system timezone Africa Harare	configure system timezone Africa Harare	Configure timezone to Africa/Harare location
configure system timezone Africa Nairobi	configure system timezone Africa Nairobi	Configure timezone to Africa/Nairobi location
configure system timezone America Anchorage	configure system timezone America Anchorage	Configure timezone to America/Anchorage location
configure system timezone America Bogota	configure system timezone America Bogota	Configure timezone to America/Bogota location
configure system timezone America Buenos_Aires	configure system timezone America Buenos_Aires	Configure timezone to America/Buenos_Aires location

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone America Chicago	configure system timezone America Chicago	Configure timezone to America/Chicago location
configure system timezone America Chihuahua	configure system timezone America Chihuahua	Configure timezone to America/Chihuahua location
configure system timezone America Denver	configure system timezone America Denver	Configure timezone to America/Denver location
configure system timezone America Godthab	configure system timezone America Godthab	Configure timezone to America/Godthab location
configure system timezone America Lima	configure system timezone America Lima	Configure timezone to America/Lima location
configure system timezone America Los_Angeles	configure system timezone America Los_Angeles	Configure timezone to America/Los_Angeles location
configure system timezone America Mexico_City	configure system timezone America Mexico_City	Configure timezone to America/Mexico_City location
configure system timezone America New_York	configure system timezone America New_York	Configure timezone to America/New_York location
configure system timezone America Noronha	configure system timezone America Noronha	Configure timezone to America/Noronha

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone America Phoenix	configure system timezone America Phoenix	Configure timezone to America/Phoenix
configure system timezone America Santiago	configure system timezone America Santiago	Configure timezone to America/Santiago
configure system timezone America St_Johns	configure system timezone America St_Johns	Configure timezone to America/St_Johns
configure system timezone America Tegucigalpa	configure system timezone America Tegucigalpa	Configure timezone to America/Tegucigalpa
configure system timezone Asia Almaty	configure system system timezone Asia Almaty	Configure timezone to Asia/Almaty location
configure system timezone Asia Baghdad	configure system timezone Asia Baghdad	Configure timezone to Asia/Baghdad location
configure system timezone Asia Baku	configure system timezone Asia Baku	Configure timezone to Asia/Baku location
configure system timezone Asia Bangkok	configure system timezone Asia Bangkok	Configure timezone to Asia/Bangkok location
configure system timezone Asia Calcutta	configure system timezone Asia Calcutta	Configure timezone to Asia/Calcutta location
configure system timezone Asia Colombo	configure system timezone Asia Colombo	Configure timezone to Asia/Colombo location

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone Asia Dhaka	configure system timezone Asia Dhaka	Configure timezone to Asia/Dhaka location
configure system timezone Asia Hong_Kong	configure system timezone Asia Hong_Kong	Configure timezone to Asia/Hong_Kong location
configure system timezone Asia Irkutsk	configure system timezone Asia Irkutsk	Configure timezone to Asia/Irkutsk location
configure system timezone Asia Jerusalem	configure system timezone Asia Jerusalem	Configure timezone to Asia/Jerusalem location
configure system timezone Asia Kabul	configure system timezone Asia Kabul	Configure timezone to Asia/Kabul location
configure system timezone Asia Karachi	configure system timezone Asia Karachi	Configure timezone to Asia/Karachi location
configure system timezone Asia Katmandu	configure system timezone Asia Katmandu	Configure timezone to Asia/Katmandu location
configure system timezone Asia Krasnoyarsk	configure system timezone Asia Krasnoyarsk	Configure timezone to Asia/Krasnoyarsk location
configure system timezone Asia Kuala_Lumpur	configure system timezone Asia Kuala_Lumpur	Configure timezone to Asia/Kuala_Lumpur location
configure system timezone Asia Kuwait	configure system timezone Asia Kuwait	Configure timezone to Asia/Kuwait location

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone Asia Magadan	configure system timezone Asia Magadan	Configure timezone to Asia/Magadan location
configure system timezone Asia Manila	configure system timezone Asia Manila	Configure timezone to Asia/Manila location
configure system timezone Asia Muscat	configure system timezone Asia Muscat	Configure timezone to Asia/Muscat location
configure system timezone Asia Rangoon	configure system timezone Asia Rangoon	Configure timezone to Asia/Rangoon location
configure system timezone Asia Seoul	configure system timezone Asia Seoul	Configure timezone to Asia/Seoul location
configure system timezone Asia Shanghai	configure system timezone Asia Shanghai	Configure timezone to Asia/Shanghai location
configure system timezone Asia Singapore	configure system timezone Asia Singapore	Configure timezone to Asia/Singapore location
configure system timezone Asia Taipei	configure system timezone Asia Taipei	Configure timezone to Asia/Taipei location
configure system timezone Asia Tehran	configure system timezone Asia Tehran	Configure timezone to Asia/Tehran location
configure system timezone Asia Tokyo	configure system timezone Asia Tokyo	Configure timezone to Asia/Tokyo location

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone Asia Yakutsk	configure system timezone Asia Yakutsk	Configure timezone to Asia/Yakutsk location
configure system timezone Atlantic Azores	configure system timezone Atlantic Azores	Configure timezone to Atlantic/
configure system timezone Australia Adelaide	configure system timezone Australia Adelaide	Configure timezone to Australia/Adelaide location
configure system timezone Australia Brisbane	configure system timezone Australia Brisbane	Configure timezone to Australia/Brisbane location
configure system timezone Australia Darwin	configure system timezone Australia Darwin	Configure timezone to Australia/Darwin location
configure system timezone Australia Hobart	configure system timezone Australia Hobart	Configure timezone to Australia/Hobart location
configure system timezone Australia Melbourne	configure system timezone Australia Melbourne	Configure timezone to Australia/Melbourne location
configure system timezone Australia Perth	configure system timezone Australia Perth	Configure timezone to Australia/
configure system timezone Europe Amsterdam	configure system timezone Europe Amsterdam	Configure timezone to Europe/Amsterdam location

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone Europe Athens	configure system timezone Europe Athens	Configure timezone to Europe/Athens location
configure system timezone Europe Belgrade	configure system timezone Europe Belgrade	Configure timezone to Europe/Belgrade location
configure system timezone Europe Berlin	configure system timezone Europe Berlin	Configure timezone to Europe/Berlin location
configure system timezone Europe Brussels	configure system timezone Europe Brussels	Configure timezone to Europe/Brussels location
configure system timezone Europe Bucharest	configure system timezone Europe Bucharest	Configure timezone to Europe/Bucharest location
configure system timezone Europe Dublin	configure system timezone Europe Dublin	Configure timezone to Europe/Dublin location
configure system timezone Europe Moscow	configure system timezone Europe Moscow	Configure timezone to Europe/Moscow location
configure system timezone Europe Paris	configure system timezone Europe Paris	Configure timezone to Europe/Paris location
configure system timezone Pacific Auckland	configure system timezone Pacific Auckland	Configure timezone to Pacific/Auckland location
configure system timezone Pacific Fiji	configure system timezone Pacific Fiji	Configure timezone to Pacific/Fiji location

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone Pacific Guam	configure system timezone Pacific Guam	Configure timezone to Pacific/Guam location
configure system timezone Pacific Honolulu	configure system timezone Pacific Honolulu	Configure timezone to Pacific/Honolulu location
configure system timezone Pacific Kwajalein	configure system timezone Pacific Kwajalein	Configure timezone to Pacific/Kwajalein location
configure system timezone Pacific Midway	configure system timezone Pacific Midway	Configure timezone to Pacific/Midway location
configure system timezone US Alaska	configure system timezone US Alaska	Configure timezone to US/Alaska location
configure system timezone US Arizona	configure system timezone US Arizona	Configure timezone to US/Arizona location
configure system timezone US Central	configure system timezone US Central	Configure timezone to US/Central location
configure system timezone US East-Indiana	configure system timezone US East-Indiana	Configure timezone to US/East-Indiana location
configure system timezone US Eastern	configure system timezone US Eastern	Configure timezone to US/Eastern location
configure system timezone US Hawaii	configure system timezone US Hawaii	Configure timezone to US/Hawaii location
configure system timezone US Mountain	configure system timezone US Mountain	Configure timezone to US/Mountain location

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure system timezone US Pacific	configure system timezone US Pacific	Configure timezone to US/Pacific location
enable	enable	Enable administrative commands
exit	exit	Exit the session
ftpput	ftpput <url> <filename> [--active]	Upload file through FTP protocol *url* STRING [ftp://username:password @hostname/path] *filename* FILENAME The file name and path to upload *active* ACTIVETYPE FTP active mode
help	help	Display an overview of the CLI syntax
history	history [limit]	Display the current session's command line history
ping	ping [-c num_echos] [-i interval] <dest>	*-c num_echos* UINT Specify the number of echo requests to be sent [5] *-i interval* UINT Wait interval seconds between sending each packet *dest* ADDRESS Host name or IP address

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
reboot	reboot [time]	Reboot this machine after a specified delay or immediately *time* UINT Time in minutes to reboot this machine [0]
resolve	resolve <dest>	Resolve an IP address on the network *dest* ADDRESS Remote ip address to resolve
restart service database **Replaces:** service database restart	restart service database	Restart the database daemon
restart service ftpd **Replaces:** service ftpd restart	restart service ftpd	Restart the FTP traffic scanning daemon
restart service httpd **Replaces:** service httpd restart	restart service httpd	Restart the HTTP traffic scanning daemon
restart service iwss_daemons **Replaces:** restart iwss_daemons	restart service iwss_daemons	Restart all IWSVA services

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
restart service logtodb **Replaces:** service logtodb restart	restart service logtodb	Restart the daemon that saves logs to database
restart service maild **Replaces:** service maild restart	restart service maild	Restart the email notification daemon
restart service metric_mgmt **Replaces:** service metric_mgmt restart	restart service metric_mgmt	Restart the metric management daemon
restart service ssh **Note:** This is a new command.	restart service ssh	Restart the SSH daemon
restart service svcmonitor **Replaces:** service svcmonitor restart	restart service svcmonitor	Restart the monitor daemon
restart service tmcmagent **Replaces:** service tmcmagent restart	restart service tmcmagent	Restart the TMCM agent

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
restart service tmsyslog **Replaces:** service tmsyslog restart	restart service tmsyslog	Restart the syslog daemon
restart service wccpd **Replaces:** service wccpd restart	restart service wccpd	Restart the WCCP daemon
restart service webui **Replaces:** service webui restart	restart service webui	Restart the tomcat daemon
show kernel iostat **Replaces:** show statistic io	show kernel iostat	Display Central Processing Unit (CPU) statistics and input/output statistics for devices, partitions and network file systems (NFS)
show kernel messages	show kernel messages	Display kernel messages
show kernel modules	show kernel modules	Display modules loaded in the kernel
show kernel parameters	show kernel parameters	Display running kernel parameters
show memory statistic **Replaces:** show statistic memory	show memory statistic	Display memory statistics

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module config all **Replaces:** show config all	show module config all	View the all the config files
show module config database **Replaces:** show config db	show module config database	View the database config files
show module config file intscan **Replaces:** show file <intscan>	show module config file intscan	View the intscan config file
show module config file IWSSPIJavascan **Replaces:** show file <IWSSPIJavascan >	show module config file IWSSPIJavascan	View the IWSSPIJavascan config file
show module config file IWSSPIProtocolFtp **Replaces:** show file < IWSSPiProtocolFtp>	show module config file IWSSPIProtocolFtp	View the IWSSPIProtocolFtp config file.

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module config file IWSSPIProtocolHttpProxy **Replaces:** show file < IWSSPIProtocolHttpProxy>	show module config file IWSSPIProtocolHttpProxy	View the IWSSPIProtocolHttpProxy config file
show module config file IWSSPIProtocolIcap **Replaces:** show file < IWSSPIProtocolIcap >	show module config file IWSSPIProtocolIcap	View the IWSSPIProtocolIcap config file
show module config file IWSSPIScanVsapi **Replaces:** show file < IWSSPIScanVsapi >	show module config file IWSSPIScanVsapi	View the IWSSPIScanVsapi config file
show module config file IWSSPISigScan **Replaces:** show file < IWSSPISigScan>	show module config file IWSSPISigScan	View the IWSSPISigScan config file
show module config file IWSSPIUrlFilter	show module config file IWSSPIUrlFilter	View the IWSSPIUrlFilter config file

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module database backup **Replaces:** show db backup	show module database backup	Display database backups
show module database password **Replaces:** show db password	show module database password	Display the database password
show module database settings **Replaces:** show db settings	show module database settings	Display the configuration of the database
show module database size **Replaces:** show db size	show module database size	Display the size of IWSVA database
show module http x-forwarded-for	show module http x-forwarded-for	Display the configuration of the XFF HTTP header module
show module ldap groupcache interval **Replaces:** show ldap groupcache interval	show module ldap groupcache interval	Display IWSVA LDAP user group membership cache interval

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module ldap ipuser_cache **Replaces:** show ldap ipuser_cache	show module ldap ipuser_cache	Display the configuration of IWSVA LDAP IP user cache. Client IP cache associates a client IP address with a user who recently authenticated from that same IP address. Any request originating from the same IP address as a previously authenticated request will be attributed to that user, provided the new request is issued within a configurable window of time (15 minutes by default for HTTP, 90 minutes for ICAP) from that authentication. The caveat is that client IP addresses seen by IWSVA must be unique to a user within that time period; thus this cache is not useful in environments where there is a proxy server or source NAT between the clients and IWSVA, or where DHCP frequently reassigns client IPs.

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module ldap ipuser_cache interval **Replaces:** show ldap ipuser_cache interval	show module ldap ipuser_cache interval	Display IWSVA LDAP IP user cache interval
show module ldap www-auth port **Replaces:** show www-auth port	show module ldap www-auth port	Display the authentication port
show module log admin **Replaces:** show log admin [log_suffix]	show module log admin [log_suffix]	View the admin log file *log_suffix* LOGSUFFIX [log_suffix] []
show module log ftp **Replaces:** show log ftp [log_suffix]	show module log ftp [log_suffix]	View the ftp log file *log_suffix* LOGSUFFIX [log_suffix] []
show module log http **Replaces:** show log http [log_suffix]	show module log http [log_suffix]	View the http log file *log_suffix* LOGSUFFIX [log_suffix] []
show module log mail **Replaces:** show log mail [log_suffix]	show module log mail [log_suffix]	View the mail log file *log_suffix* LOGSUFFIX [log_suffix] []

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module log postgres **Replaces:** show log postgres	show module log postgres	View the postgres log
show module log tmudump **Replaces:** show log tmudump	show module log tmudump	View the tmudump log file
show module log update **Replaces:** show log update [log_suffix]	show module log update [log_suffix]	View the update log file *log_suffix* LOGSUFFIX [log_suffix] []
show module metrics ftp **Replaces:** show metrics ftp	show module metrics ftp	Display IWSVA ftp performance metrics
show module metrics http **Replaces:** show metrics http	show module metrics http	Display IWSVA http performance metrics
show module ntp schedule **Replaces:** show ntp schedule	show module ntp schedule	Display the scheduled NTP server configuration

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show module webui port **Replaces:** show webserver port	show module webui port	Display Web server port settings
show network arp **Replaces:** show arp [dest]	show network arp [dest]	Display system arp tables *dest* <u>ADDRESS</u> Remote IP address to arp
show network bonding <bonding name>	show network bonding <bonding name>	Display bonding settings If <bonding name> is missing, all bonding settings display. If <bonding name> is specified, specified bonding settings display.
show network bridge redirect ftpports **Replaces:** show redirect ftpports	show network bridge redirect ftpports	Display the FTP redirection port numbers
show network bridge redirect httpports **Replaces:** show redirect httpports	show network bridge redirect httpports	Display the HTTP redirection port numbers
show network bridge redirect httpsports **Replaces:** show redirect httpsports	show network bridge redirect httpsports	Display the HTTPS redirection port numbers

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show network bridge stp **Note:** This is a new command.	show network bridge stp	Display the bridge STP settings
show network capture **Replaces:** show capture [filename]	show network capture [filename]	Display packets captures *filename* STRING [filename] []
show network connections <all/listening> <all/tcp/udp> **Replaces the following commands:** show connections show daemons **Note:** Additional parameters available in new command.	show network connections <all/listening> <all/tcp/udp>	Display system connections or daemons. For example, execute "show network connections listing" to display which daemons are running.
show network conntrack **Replaces:** show conntrack	show network conntrack	Display state tracked connections
show network conntrack expect **Replaces:** show conntrack expect	show network conntrack expect	Display state expected connections

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show network data interface **Replaces:** show ip address	show network data interface	Display network address
show network dns **Replaces:** show ip dns	show network dns	Display network dns servers
show network ethernet **Replaces:** show ethernet <ethname>	show network ethernet <ethname>	Display Ethernet card settings *ethname* IFNAME Interface name
show network firewall filter **Replaces:** show firewall filter	show firewall filter	Display firewall filter
show network firewall nat **Replaces:** show firewall nat	show firewall nat	Display firewall NAT
show network gateway **Replaces:** show ip gateway	show network gateway	Display network gateway

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show network hostname **Replaces:** show hostname	show network hostname	Display network hostname
show network interfaces **Replaces:** show interfaces	show network interfaces	Display network interface information
show network interfaces status Replaces: **Note:** This is a new command.	show network interfaces status	Display the link status of the network card
show network interfaces status once **Note:** This is a new command.	show network interfaces status once	Display the link status of the network card once
show network interfaces statistic **Note:** This is a new command.	show network interfaces statistic	Display the link status of the network card
show network lanbypass **Note:** This is a new command.	show network lanbypass	Displays the current configuration status of LAN-bypass function If lanbypass used, it would show one of the following states: on / off / auto.

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show network mgmt interface **Replaces:** show mgmt ip address show mgmt status	show network mgmt interface	Display the status and address information
show network ping **Replaces:** show ping show ping mgmt	show network ping	Display data and management status
show network portgroup	show network portgroup	Display current port group settings
show network route **Replaces:** show ip route	show network route	Display network routing table
show network sockets **Replaces:** show open sockets	show network sockets	Display open network socket statistics
show process library	show process library <pid>	A library call tracer *pid* UINT <pid>
show process stack	show process stack <pid>	Print a stack trace of a running process *pid* UINT <pid>

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show process [target]	show process [target]	Display process information *target* STRING [optional name/ID with wildcard support] []
show process top	show process top	Display information about running processes
show process trace	show process trace <pid>	Trace system calls and signals *pid* UINT <pid>
show service ssh **Replaces:** show ssh	show service ssh	Show status of SSH service
show storage partition **Replaces:** show disk partition [partition] show disk partition readable [partition]	show storage partition [partition]	Report filesystem usage in readable format only *partition* STRING [optional partition] []
show storage space **Replaces:** show disk space [target] show disk space readable [target]	show disk space [target]	Report file space usage in readable format only *target* STRING [optional directory or filename] [/]

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show storage statistic **Replaces:** show statistic disk	show storage statistic	Display disk statistics
show system configuration	show system configuration	Display summary information of running configuration
show system configuration [-verbose] **Replaces:** show running configuration -verbose	show system configuration [-verbose]	Display detailed information of running configuration
show system date Replaces: show date	show system date	Display current date/time
show system ha **Note:** This is a new command.	show system ha	Display HA information, such as: Cluster name, Description, HA mode, Deployment mode, Cluster IP address, Preemption, Member list, Role, Localhost, Hostname, IP address, Weight
show system hwmonitor **Note:** This is a new command.	show system hwmonitor	Display hardware monitoring information.

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show system hwmonitor interval **Note:** This is a new command.	show system hwmonitor interval	Show current polling interval value.
show system hwmonitor sel **Note:** This is a new command.	show system hwmonitor sel	Shows the hardware event log information as a base for sending SNMP traps.
show system hwmonitor sensor **Note:** This is a new command.	show system hwmonitor sensor	Shows all the information gathered from sensors.
show system keyboard	show system keyboard	Display default keyboard table
show system openfiles **Replaces:** show open files [target]	show system openfiles [target]	Display open files *target* STRING [optional directory or filename] []
show system timezone **Replaces:** show timezone	show timezone	Display the timezone on IWSVA
show system uptime **Replaces:** show uptime	show system uptime	Show how long the system has been running

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show system version **Replaces:** show version	show system version	Display IWSVA version
shutdown	shutdown [time]	Shutdown this machine after a specified delay or immediately *time* UINT Time in minutes to shutdown this machine [0]
start service database **Replaces:** service database start	start service database	Start the database daemon
start service ftpd **Replaces:** service ftpd start	start service ftpd	Start the FTP traffic scanning daemon
start service httpd **Replaces:** service httpd start	start service httpd	Start the HTTP traffic scanning daemon
start service logtodb **Replaces:** service logtodb start	start service logtodb	Start the daemon that saves logs to database
start service maild **Replaces:** service maild start	start service maild start	Start the email notification daemon

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
start service metric_mgmt **Replaces:** service metric_mgmt start	start service metric_mgmt	Start the metric management daemon
start service ssh **Replaces:** enable ssh	start service ssh	Enable the sshd daemon
start service svcmonitor **Replaces:** service svcmonitor start	start service svcmonitor	Start the monitor daemon
start service tmcmagent **Replaces:** service tmcmagent start	start service tmcmagent	Start the TMCM agent
start service tmsyslog **Replaces:** service tmsyslog start	start service tmsyslog	Start the syglog daemon
start service wccpd **Replaces:** service wccpd start	start service wccpd	Start the WCCP daemon

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
start service webui **Replaces:** service webui start	start service webui	Start the tomcat daemon
start shell **Replaces:** admin shell	start shell	Administrative shell access
start task database backup **Replaces:** admin db backup	start task database backup	Back up your database
start task database reindex **Replaces:** admin db reindex	start task database reindex	Reindex the IWSVA database
start task database restore **Replaces:** admin db restore [filename]	start task database restore [filename]	Restore your database from a backup
start task database truncate **Replaces:** admin db truncate <DATE_FIELD>	start task database truncate <DATE_FIELD>	Truncate the IWSVA database

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
start task database vacuum **Replaces:** admin db vacuum	start task database vacuum	Vacuum the IWSVA database
start task capture interface **Replaces:** capture interface <interface> [-h host] [-p port]	start task capture interface <interface> [-h host] [-p port]	Capture network interface traffic *interface* IFNAME interface to capture packets *-h* host IP_ADDR filter by IP address *-p* port UINT filter by port number
start task monitor ftp **Replaces:** monitor ftp	start task monitor ftp	Monitor the FTP log
start task monitor http **Replaces:** monitor http	start task monitor http	Monitor the HTTP log
stop process	stop process <pid>	Stop a running process *pid* UINT <pid>
stop process core	stop process core <pid>	Stop a running process and generate a core file *pid* UINT <pid>

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
stop service database **Replaces:** service <database> stop	stop service database	Stop the database daemon
stop service ftpd **Replaces:** service <ftpd> stop	stop service ftpd	Stop the FTP traffic daemon
stop service httpd **Replaces:** service httpd stop	stop service httpd	Stop the HTTP traffic daemon
stop service logtodb **Replaces:** service logtodb stop	stop service logtodb	Stop the daemon that saves logs to database
stop service maild **Replaces:** service maild stop	stop service maild	Stop the email notification daemon
stop service metric_mgmt **Replaces:** service metric_mgmt stop	stop service metric_mgmt	Stop the metric management daemon
stop service ssh **Replaces:** disable ssh	stop service ssh	Disable the sshd daemon

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
stop service svcmonitor **Replaces:** service svcmonitor stop	stop service svcmonitor	Stop the monitor daemon
stop service tmcmagent **Replaces:** service tmcmagent stop	service stop tmcmagent	Stop the TMCM agent
stop service tmsyslog **Replaces:** service tmsyslog stop	stop service tmsyslog	Stop the syslog daemon
stop service wccpd **Replaces:** service wccpd stop	stop service wccpd	Stop the WCCP daemon
stop service webui **Replaces:** service webui stop	stop service webui	Stop the tomcat daemon
traceroute	traceroute [-h hops] <dest> [-n]	TraceRoute *-h hops* UINT Specify maximum number of hops *dest* ADDRESS Remote system to trace *-n* DASHN Do not resolve hostname []

TABLE 11-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
wget	wget <url> <path>	Download file through HTTP/FTP protocols *url* STRING [http://username:password@hostname/path] *path* FILENAME The local path to download file

Chapter 12

Reports, Logs, and Notifications

This chapter describes how administrators can get timely information about their gateway security through InterScan Web Security Virtual Appliance (IWSVA) reports, logs, and notifications.

Topics in this chapter include the following:

Summary Reports

The IWSVA console opens to the Summary screen that displays the System Dashboard with real-time, dynamic system information. Other available reports display static information. Tabs on the Summary screen provides access to the following:

- *Real-time Statistics*
- *Scanning Activity*
- *URL Activity*
- *Spyware Activity*
- *Security Risk Reporting*
- *Hardware Status*

Real-time Statistics

IWSVA provides dynamic statistics where the administrator can view the "real-time" information about the IWSVA system. These statistics are displayed as graphs in the System Dashboard tab of the Summary page and include the following:

- *Virus and Spyware Trend Display*
- *Component Update Status Display*
- *Hard Drive Display*
- *Bandwidth Display*
- *Concurrent Connections Display*
- *CPU Usage Display*
- *Physical Memory Usage Display*

The "Virus and Spyware Trend" dashboard displays the latest information as to when the report was generated. The information displayed is not updated in real time as in the other dynamic real-time reports of the Summary (System Dashboard tab) screen.

Note: If the system time is adjusted backward (either manually or through automatic network time server synchronization), IWSVA will stop gathering real-time statistics information. To have IWSVA collect real-time statistics information, you must restart the metric management daemon. Type the following commands in the CLI:

```
stop service metric_mgmt
start service metric_mgmt
```

Virus and Spyware Trend Display

This is a static display that shows the rate at which viruses and spyware are being detected by IWSVA. (You can specify threshold alerts so that you are notified of a critical level of virus and/or spyware "hits.") The rate is based on a seven-day period and "hits" are recorded daily. Therefore, a new display is started every seven days. The display does not include the names of users involved.

Note: Because each day's virus and spyware data is represented by a single point on the display, IWSVA cannot start graphing data until there are two points, or two days worth of data available.

The information in the Virus and Spyware display is for the entire IWSVA.

Component Update Status Display

This is a static display that shows the current version of IWSVA components (such as the scanning engine and virus pattern) and the dates they were last updated. To manually update the components, click **Update** to display the Manual Update screen. See *Manual Updates* on page 4-11 for more information.

Hard Drive Display

This is a static display that shows the status of the disk(s) used by IWSVA for its system files, quarantine space, temporary space, and logs. The Hard Drive display can monitor up to 12 disks.

If the database resides on the same drive as any of these directories, then the database disk usage is also included in the display. The scale along the Y-axis ranges from 10 to 100 percent.

You can specify threshold alert values and the frequency of alerts so that you are notified when any of the hard disk statuses reach a critical level. IWSVA can send these alerts either through email, SNMP trap/notification (if enabled), or both. SNMP traps are sent when a configured threshold value is met.

Bandwidth Display

This is a dynamic display that shows the bandwidth usage of both inbound and outbound traffic for HTTP and FTP. IWSVA recognizes traffic in terms of requests and responses. Therefore, the display interprets all requests as outbound traffic and all responses as inbound traffic. From this display, you can view any potential bandwidth problems.

The display shows ten data points that give the graph a history of five to ten minutes of activity. This activity is only monitored for the local IWSVA device. With the ideal refresh rate being between 30 and 60 seconds, the display has a default refresh rate of 30 seconds.

Clicking the 1-day or 30-day button opens a window that shows a static chart with one or 30 days of usage, respectively. IWSVA retrieves this information from the database. If the database does not contain enough data, the display shows the data that is available.

Note: The 30-day display option shows each day's bandwidth usage data by a single point. For the 1-day display option, the screen shows the bandwidth usage for each hour of the day by a single point. IWSVA cannot start graphing data until there are at least two points worth of data available.

You can specify threshold alert values and the frequency of alerts so that you are notified when a bandwidth usage reaches a critical level. IWSVA can send alerts either through email, SNMP trap/notification (if enabled), or both. See *Email Notification Settings* on page 12-38.

Note: The bandwidth setting should be very high—above "out of normal range" values to avoid frequent alerts.

Concurrent Connections Display

This dynamic display shows concurrent connections usage for HTTP(s) in purple and FTP in orange. It shows the number of connections and connection time (in seconds.)

CPU Usage Display

This is a dynamic display that shows CPU utilization on the local system. In the case of multiple CPUs, the display shows the average IWSVA usage across all CPUs. It does this by displaying a single line for all CPU utilization. IWSVA determines the CPU utilization based on CPU cycles used, CPU cycles used by IWSVA, and total CPU cycles used by the backend, CPU-monitoring API.

By default, IWSVA samples the CPU usage each second for two minutes, giving you 120 data points. In the init file, you can change the default refresh rate.

Clicking the 1-day or 30-day button opens a window that shows a static chart with one or 30 days of CPU usage, respectively. IWSVA retrieves this information from the database. If the database does not contain enough data, then the display shows the data that is available.

Note: The 30-day display option shows each day's CPU usage data by a single point. For the 1-day display option, the screen shows the CPU usage for each hour of the day by a single point. IWSVA cannot start graphing data until there are at least two points worth of data available.

Physical Memory Usage Display

This is a dynamic display that shows the amount of physical memory used by the local IWSVA server.

By default, IWSVA samples the physical memory usage each second for two minutes, giving you 120 data points. In the init file, you can change the default refresh rate.

Clicking the 1-day or 30-day button opens a window that shows a static chart with one or 30 days of physical memory usage, respectively. IWSVA retrieves this information from the database. If the database does not contain all the data, the display shows the data that is available.

Note: The 30-day display option shows each day's physical memory usage data by a single point. For the 1-day display option, the screen shows the physical memory usage for each hour of the day by a single point. IWSVA cannot start graphing data until there are at least two points worth of data available.

Scanning Activity

Activities pertaining to scanning are available from the **Scanning** tab. They include the following:

- Enabling and disabling HTTP and FTP traffic (available from all **Summary** page tabs)
- Access links to Trend Micro's Web threat protection sites (available from all **Summary** page tabs)
- Displaying malware names and frequency of occurrence in scanning results by selected time period
- Top 5 Virus/Malware Risk (last 7 days) based on IP Address /Host name/User name
- Refreshing scanning results

The **Scanning** tab displays the names of top five most detected virus/malware and devices at risk. In addition, you can also view scanning results by a selected time period.

URL Activity

Activities pertaining to URL activity are available from the **URL** tab. This screen includes the top URLs/categories/phishing sites blocked for the past seven days and URL activity by selected time period displays of the following items:

- Most blocked URLs
- Most blocked URL categories
- Most blocked phishing sites
- URL activity summary

Spyware Activity

Activities pertaining to spyware activity are available from the **Spyware** tab. This tab displays scanning information about the following:

- **Top 5 Detected Spyware (last 7 days)**—This section gives the spyware name and the option to add it to the exceptions list.
- **Top 5 Spyware Risks (last 7 days)**—This sections lists the User ID from which the risk initiates.
- **Scanning results for (Today, Past week, or Past month)**—This sections lists the spyware name and frequency of occurrence.
- **Cleanup results for (Today, Past week, or Past month)**—This section lists the malware type and the number of each type cleaned.

Security Risk Reporting

Activities pertaining to security risk reporting are available from the **Security Risk Report** tab. Security Risk Reporting displays information for the past week or the past 28 days on different types of malicious activity. A comprehensive graph provides an "at-a-glance" view of multiple, color-coded threats.

Data from this report (listed by day or week) can be exported in CSV format or printed. The type of threats tabulated here include:

- **Malware**—such as viruses, macros, Trojans, IntelliTrap detections, and others
- **Spyware/grayware**—such as spyware, grayware, and ActiveX
- **Pharming**—such as those reported by Web Reputation
- **Phishing**—such as those reported by Web Reputation and the phishing pattern
- **Unauthorized Web acces**s—such as URL filtering and offending URLs detected by Web Reputation
- **Instant Messaging**—detected by IntelliTunnel

Hardware Status

The Hardware Status feature provides the administrator with the ability to monitor hardware information about fans, voltage, temperature, etc. on Intelligent Platform Management Interface (IPMI)-enabled devices.

Note: IWSVA hardware monitoring is only compatible with the Baseboard Management Controller (BMC) with Intelligent Platform Management Interface (IPMI) v2.0 support installed on bare metal.

Administrators can query the hardware status information using the IWSVA Web console or by SNMP request. If SNMP trap is enabled, an alert will be sent when system events are detected, such as "temperature threshold exceeded", "voltage threshold exceeded", etc.

Alerts can be sent to notify administrators of any problems. They are configured at: **Notification > SNMP Notifications Settings > Hardware monitoring events** (check box).

The following provides a brief description of the options available on the Hardware Status screen:

- **Interface Status**—Icons shown *Table 12-1* represent the status of the interfaces:

TABLE 12-1. Interface Status Indicators

ICON	DESCRIPTION
	Link not detected. Could be an empty port, cable may be loose or broken, or the peer machine may be down.
eth0	Link OK
eth1 ⚠	Link error

TABLE 12-1. Interface Status Indicators (Continued)

ICON	DESCRIPTION
eth1	Link disabled
D	Data interface
M	Management interface
H	High availability interface

- **Hardware Type**—shows Voltage, Fan, CPU, Storage and Temperature statistics
- **Status**—shows the current status of the hardware. Usually it shows **"**Normal,**"** but if an abnormal event occurs, it displays Critical or Failed, depending on the event. The five available status are:
  - **Normal**—Component status is ok
  - **Warning**—Component status is compromised
  - **Critical**—Component status is in danger of failing
  - **Failed**—Component is not working
  - **Unknown**—No component information is available
- **Sensor Information**—displays information about the status of the type of hardware monitored.

SNMP Queries and Traps

Administrators can poll the hardware status using SNMP queries and receive alerts through SNMP traps. To do this, administrators need import the hardware-monitoring MIB file into an SNMP tool like iReasoning MIB Browser.

IWSVA also supports two standard MIB files for network interface card statistics:

- RFC1213-MIB
- HOST-RESOURCES-MIB

These are available from:

`http://www.simpleweb.org/ietf/mibs/`

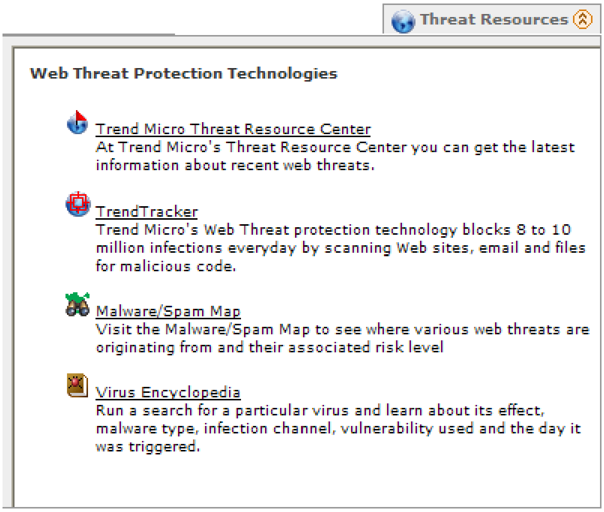
The third Trend Micro-specific MIB for hardware events monitoring is:
TM-HWMONITOR-MIB

located on the Trend Micro download site at:
`http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=1747&regs=NABU&lang_loc=1#undefined`

To receive traps from IWSVA, administrators need configure the SNMP trap destination at **Administration > Network Configuration > SNMP Settings**.

Accessing Additional Web Threat Information

From the **Threat Resources** drop-down list in the upper right corner of the **Summary** page, you can access the links to Trend Micro’s Web threat protection sites to learn more about the latest Web threats, research from where various Web threats are originating, access Trend’s virus encyclopedia, and see real-time Web and email malware statistics.See Enabling HTTP Scanning and Applets and ActiveX Security on page 7-2 to view the **Threat Resources** drop-down list.



Threat Resources

Web Threat Protection Technologies

Trend Micro Threat Resource Center
At Trend Micro's Threat Resource Center you can get the latest information about recent web threats.

TrendTracker
Trend Micro's Web Threat protection technology blocks 8 to 10 million infections everyday by scanning Web sites, email and files for malicious code.

Malware/Spam Map
Visit the Malware/Spam Map to see where various web threats are originating from and their associated risk level

Virus Encyclopedia
Run a search for a particular virus and learn about its effect, malware type, infection channel, vulnerability used and the day it was triggered.

FIGURE 12-1. Web threat protection technologies that can be accessed in IWSVA

Introduction to Reports

IWSVA can generate reports about virus and malicious code detections, files blocked, URLs accessed and DCS cleanups. You can use this information about IWSVA program events to help optimize program settings and fine tune your organization's security policies.

You can configure and customize reports. For example, IWSVA allows you to generate reports for all or specific user(s), all or specific group(s), either on demand (in real time) or on a scheduled basis.

In addition, for scheduled reports, you can create report templates based on user(s)/group(s) or report type. To allow you to share the selected report information with those who need it, IWSVA can send the generated report through email as file attachments.

Types of Reports

IWSVA can generate the following categories of reports:

- **Violation-event reports:** Reports about virus detections, policy violations, blocked URLs, and monitored URLs
- **Spyware/Grayware reports:** Reports about spyware detections
- **Cleanup reports:** Reports about DCS cleanup attempts requested by IWSVA
- **Traffic reports:** Reports about Web browsing activity, the most popular Web sites and downloads, and other details about Web browsing activity
- **URL filtering category reports:** Reports about a main category or selected sub-categories
- **Individual/per user reports**

The following sections describe all available reports.

Violation-event Reports

IntelliTrap is used to detect potentially malicious code in real-time, compressed executable files that arrive with HTTP(s) data. When IntelliTrap detects a malicious executable file, the following detections appears in Violation-event reports:

- Riskiest URLs by viruses detected
- Users with most requests for malicious URLs
- Most violations by user
- Most violations by group
- Most blocked URL categories
- Most monitored URL categories
- Most warned (including warned and continued) URL categories
- Most blocked Applets and ActiveX objects
- Most blocked URLs
- Most monitored URLs
- Most blocked URLs by day of the week
- Most blocked URLs by hour

- Most warned (including warned and continued) URLs
- IntelliTunnel report

Summary Reports

- Most blocked URLs by day of the week
- Most blocked URLs by hour

Spyware/Grayware Reports

- Spyware/grayware detection by category
- Top spyware/grayware detections
- User with most Spyware/Grayware infections

Cleanup Reports

- Cleanup events by category
- Top cleanup events by name
- Most infected IP addresses

Note: Cleanup reports require the installation of the Damage Cleanup Services (DCS) component and the registration of IWSVA and DCS (Administration > IWSVA Configuration > Register to DCS).

Traffic Reports

For traffic reports, you need to enable "Log HTTP/HTTPS/FTP access events" in **Logs > Log Settings**.

Traffic reports might take a long time to generate; that is, up to a few hours for large sites with extensive access logs.

- Most active users
- Most popular URLs
- Most popular downloads
- Most popular search engines

- Top categories (weighted)

Summary Reports

- Daily traffic report
- Activity level by day of the week
- Activity level by hour

URL Filtering Category Reports

- Most active users
- Most active URLs
- Most monitored users
- Most monitored URLs
- Most warned (including warned and continued) users
- Most warned (including warned and continued) URLs

Individual/per User Reports

- Overview report
- Most popular sites visited by user*
- Most blocked URL categories by user
- Most monitored URL categories by user
- Most warned (including warned and continued) URL categories by user
- Most blocked URLs by user
- Most monitored URLs by user
- Most warned (including warned and continued) URLs by user

Summary Reports

- Overview report
- URL activity by user*

* Log HTTP/HTTPS/FTP access events must be enabled in **Logs > Log Settings**

Report Settings

When generating a real-time report or setting up scheduled reports, you need to specify the information in the following sections:

- Report Scope (Users and Groups) on page 12-15
- Generate Reports by Protocol on page 12-15
- Type and Number of Report Records on page 12-16
- Options on page 12-16
- Additional Report Settings on page 12-16

Report Scope (Users and Groups)

Select the user(s) and or group(s) for which you want to generate a report. Options include:

- **All users**: All clients accessing the Internet through IWSVA
- **Specific user(s)**: Clients with specific IP addresses, host names, or LDAP directory entries
- **All groups**: All groups in the LDAP directory; if using the IP address or host name identification method, then “All groups” is equivalent to “All users”
- **Specific group(s)**: Either specified LDAP groups or a range of IP addresses

When generating reports for specific users or groups, the user selection method is determined by the method configured under **HTTP > Configuration > User Identification | User Identification** tab. For more information about user identification, see Configuring the User Identification Method starting on page 6-5.

Generate Reports by Protocol

You can select to generate reports based on selected Web protocols (**HTTPS**, **HTTP**, or **FTP**). For example, you can select to generate reports for HTTPS traffic to check detected threats through HTTPS connections.

Type and Number of Report Records

IWSVA allows you to specify the number of records shown in different reports. For example, you can configure the number of users to be listed on the “Most active users” Web traffic report. The default number of records for all reports is 10. The maximum number of report records allowed is 99.

Options

IWSVA can present program information in either bar, stacked bar or line charts. Different chart shading for URLs or downloads blocked by IWSVA versus successful requests can also be used.

Additional Report Settings

For real-time reports, specify the time period the report covers.

When setting up a scheduled report, there are some additional settings:

- Send a copy of the report to a specific person or email distribution list after the report has been generated
- Run the reports at a specific time and day
- “Enable” the report to run at the scheduled time

Generating Reports

Real-time Reports

IWSVA enables you to generate reports in real time for either all or a subset of the clients accessing the Internet. You can save the generated real-time report in PDF or CVS format (click the corresponding link on the upper left corner in the report screen).

To configure real-time reports:

1. Click **Reports > Real-Time Reports** in the main menu.
2. Under “**Time period**,” select a time period for the report (either **All Dates**, **Today**, **Last 7 days**, **Last 30 days**). Or click **Range** to generate a report in a given time range, and then select the **From** and **To** dates.

3. Under **Report by**, select the users for which the report is generated—either **All users**, **Specific user(s)**, **All groups**, or **Specific group(s)**. For more information about running reports for specific users or groups, see *To select specific group(s):* and To select specific user(s): starting on page 12-18.
4. Under **Generate Report by Protocol**, select the Web protocol for which you want to generate a report.
5. Under **Report Type**, select the report type(s) and enter the desired report record number(s).

Note: IWSVA groups multiple report parameters into a single report, with each report parameter having its own section.

6. Under **Options**, select the chart type from the menu. To denote blocked traffic from unblocked traffic using different shading, select "**Distinguish blocked from unblocked traffic**."
7. Click **Generate Report**.

   Click **Reset** to reset the form to the default values.

The following table provides information about the parameters that can comprise a report:

TABLE 12-2. Report Parameter Availability Depends on the Report Type

REPORT BY	REPORT PARAMETERS INCLUDED
All users	Includes all listed report parameters except for "Individual user reports"
Specific users	Includes only the "Individual user reports" parameters

TABLE 12-2. Report Parameter Availability Depends on the Report Type

REPORT BY	REPORT PARAMETERS INCLUDED
All groups or Specific groups	The following reports are enabled: - Most violations by group* - Most blocked URL categories* - Most monitored URL categories* - Most warned (including warned and continued) URL categories - Most blocked Applets and ActiveX objects - Most blocked URLs* - Most monitored URLs* - Most blocked URLs by day of the week* - Most blocked URLs by hour*
* For Web Reputation (including anti-pharming and anti-phishing), blocked sites appear in these reports. But to find a blocked site, the information is only in "Most blocked URLs."	

To select specific group(s):

1. Click **Reports >Real-time Reports** in the main menu.
2. Under **Report by**, select **Specific group(s)**, and then click **Select**.

   When you click **Select** on **Specific group(s)** (**Reports > Real-time Reports > Report by**), the **Select Groups** pop-up screen opens according to the configured user identification method (**HTTP > Configuration > User Identification | User Identification**).
3. Type the IP address range (or search for a group name in your LDAP directory if using the "User/group name authentication" identification method).
4. Click **Add**.
5. After adding all the groups, click **Save**.

To select specific user(s):

1. Click **Reports > Real-time Reports** in the main menu.
2. Under **Report by**, select **Specific user(s)**, and then click **Select**.

When you click **Select** on **Specific user(s)** (**Reports > Real-time Reports > Report by**), the **Select Users** pop-up screen opens according to the setting made in the user identification method (**HTTP > Configuration > User Identification | User Identification**).

3. Type the **IP address**, **Host name** or search for a user name in your LDAP directory if using the "User/group name authentication" identification method.
4. Click **Add**.
5. After adding the users to include in the report, click **Save**.

Scheduled Reports

You can configure IWSVA to generate scheduled reports on a daily, weekly, or monthly basis.

To configure scheduled reports:

1. Create a new report template in the **Reports > Report Template** (see *Scheduled Report Templates* on page 12-20).
1. Click **Reports > Scheduled Reports > Daily Reports | Weekly Reports | Monthly Reports** from the main menu.
2. Click **Add** or a report name to edit it.
3. Enter a name for the new report. Set the time and/or date to generate the scheduled report.
4. Under **Report template,** select a template from the drop down list.

Note: Template reports must exist before you can configure a new scheduled report profile. For more information, see: Scheduled Report Templates on page 12-20.

5. Select **Email this report** and the attachment format, and type the email address(es) to which IWSVA should send the generated report as a file attachment. You must also enter the **From** and **Subject** fields. Separate multiple email addresses with commas.
6. Click **Save**.

To delete a scheduled report:

1. Click **Reports > Scheduled Reports > Daily Reports | Weekly Reports | Monthly Reports** in the main menu.
2. Select the report setting to remove and then click **Delete**.

Note: Deleting a scheduled report will not remove the associated report template.

Scheduled Report Templates

To define what content is to be included in a report and customize report format, IWSVA allows you to configure report templates to generate only the reports that you want to distribute to specific recipients. After you have created a report template, you can apply it to a scheduled report profile. IWSVA generates the report and distributes it to specific recipients based on the settings in the scheduled report profile.

You can create different report templates for daily, weekly, and monthly reports. In addition, report templates can be reused and changes made to a template are automatically reflected in the associated reports. The **Copy** function allows you to create new report templates quickly by adjusting the settings copied from another template.

To configure a scheduled report template:

1. Click **Reports > Report Template** from the main menu.
2. Click **Add** or click a template name to edit an existing one.
3. Enter the **Template Name** for a new template.
4. Under **Generate Report for**, select the users for which the report is generated—either **All users**, **Specific user(s)**, **All groups**, or **Specific group(s)**. For more information about running reports for specific users or groups, see *To select specific group(s):* and To select specific user(s): starting on page 12-18.
5. Under **Report Type**, select the report type and enter the desired report parameter(s).
6. Under **Options**, select the chart type from the menu. To denote blocked traffic from unblocked traffic using different shading, select "**Distinguish blocked from unblocked traffic**."
7. Click **Save**.

To create a new report template based on the settings of an existing template:

1. Click **Reports > Report Template** from the main menu.
2. Select the name of the template you want to copy. Click **Copy**. The **Add Template** screen displays with the settings of the template you have selected.
3. Enter a different name in the **Template Name** field and make changes to the template if required.
4. Click **Save**.

Saved Scheduled Reports

When a scheduled report is generated, IWSVA sends the report to specified recipients and saves a copy to the database. You can view or download the saved report under **Reports > Scheduled Report > Daily Reports | Weekly Reports | Monthly Reports** and click the **Saved Reports** tab. You can configure the number of saved reports IWSVA is to store in the database (refer to Customizing Reports starting on page 12-21).

To download a saved scheduled report:

1. Click **Logs > Scheduled Report > Daily Reports | Weekly Reports | Monthly Reports** and click the **Saved Report** tab.
2. Click a report name to display the report.
3. You can save the report in HTML format using the save feature in your Web browser or click to save the report in **CSV** or **PDF** format on your computer.

To delete a saved scheduled report:

1. Click **Reports > Scheduled Reports > Daily Reports | Weekly Reports | Monthly Reports** in the main menu.
2. Click **Saved Reports** tab.
3. Select the reports to remove and then click **Delete**.

Customizing Reports

You can configure IWSVA to archive scheduled reports. The default path for archiving reports is `/var/iwss/report` but can be modified. The default configuration is to archive 60 daily reports, 20 weekly reports, and four monthly reports before deleting them from the server, but you can configure the number of scheduled reports to save.

To customize the report data maintenance settings:

1. Click **Reports > Customization** in the main menu.
2. Under **Report Archives**, type the following information in the fields provided:
   a. **Archive Directory** to save the reports (the default is `/var/iwss/report`)

   > **Note:** When changing the **Archive Directory**, the folder must exist on the IWSVA device before it is entered into the **Report Customization** page. In order to view reports already generated, copy them over to the new folder.

   b. Number of scheduled reports to save:
      - **Daily reports** (default is 60)
      - **Weekly reports** (default is 20)
      - **Monthly reports** (default is 4)
3. Click **Save**.

Introduction to Logs

There are two types of logs available with IWSVA: reporting logs and system logs.

Reporting logs provide program event information, and the IWSVA Web console can be used to query and view them. These logs include:

- Virus
- URL blocking
- URL filtering
- Performance
- Spyware/Grayware
- System events
- URL access

System logs contain unstructured messages about state changes or errors in the software, and are only visible by viewing the log file—they cannot be seen from the Web console. System logs include the following logs:

- HTTP scan
- FTP scan
- Mail delivery daemon
- Administration, Update, and Audit trails

The IWSVA database stores all log data, but log data can also be stored in text log files for backward compatibility with previous IWSVA versions or used with an external reporting tool. Storing the log data in text log files provides redundancy to verify that the database is properly updated. Trend Micro recommends using the database as the only storage location for log data.

In addition, IWSVA provides syslog capabilities. This allows you to configure IWSVA to send specified logs to one or more external syslog servers.

Options for Recording Data

IWSVA uses data from reporting logs to generate reports. You can configure IWSVA to write reporting log data to both the database and text logs, only to the database, or only to the text log. If you choose the text-only option, then neither reports nor logs can be viewed from within the IWSVA user interface. In this case, you can only review the logs by directly opening the generated text files.

Configure reporting log options in the IWSVA Web console under **Logs > Log Settings** (see Log Settings starting on page 12-32 for more information).

There is a performance penalty for enabling the access log (**Log HTTP/HTTPS/FTP access events** is disabled by default). By default, access logging is disabled. In order to obtain reports for user access, you must enable access logging by selecting **Log HTTP/HTTPS/FTP access events** in the **Logs > Log Settings > Reporting Logs** screen.

If you do not enable access logging, many reports on user activities will not available. Moreover, if IWSVA is configured as an upstream proxy, valuable data on user activities might not be available. If you want IWSVA to summarize all Web-related activities, enable the access log under the **Options** section in **Logs > Log Settings > Reporting Logs**.

Note: When the access log is enabled, the IWSVA service is restarted. During the restart, a router might take up to 30 seconds to recognize IWSVA again, during which time the router does not redirect packets.

Querying and Viewing Logs

The IWSVA Web console provides tools to query log files.

Audit Log

The audit log contains information that describes any configuration changes that users make to the application. For instance, after a migration or rollback procedure is activated by a user, an entry recording the migration activity is created in the audit log.

To view the audit log:

1. Click **Logs > Log Query > Audit Log** in the main menu.
2. Under **Time period**, select the time for which you want a report generated.

   Click **Range** to view the virus log in a given time range, then select the start and end dates.
3. Under **User(s)**, select the user(s) for which you want to view log entries. Click **Add** (or **Add All** for all users listed). To remove user(s) from the right list box, click **Remove** (or **Remove All** for all users listed).
4. Under the **Sort by** section, select an option by which to sort the display log. The options are "User" and "Date."
5. Click **Show Log**. The **Audit Log** screen opens.
6. Click **Refresh** to update the screen.

Cleanup Log

The cleanup log contains information returned by DCS after it performs a cleanup of the client machine. If no response is returned from a DCS server, there is no entry for that clean up request.

To view the virus log:

1. Click **Logs > Log Query > Cleanup Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Malware cleaned**, select the malware name(s).

   Highlight the names to add, and then click **Add** (or **Add All** for all viruses listed). To remove malware name(s) from the right list box, click **Remove** (or **Remove All** for all malware names listed).

   Under some circumstances, DCS is unable to connect to a client machine when IWSVA sends the cleanup request. Because no malware is cleaned during these attempts, querying the cleanup log by malware name does not display any information. To view logs about cleanup attempts when DCS could not successfully connect to the client machine, select **Show connection failure events**.
4. Under the **Sort by** section, select a sort option (Malware, Date, IP address, Action, Type, or Subtype).
5. Click **Show Log**. The **Cleanup Log** viewing screen opens.
6. Click **Refresh** to update the screen.

FTP Get Log

The FTP Get log contains all FTP Get transaction information, including user ID, date, FTP transfer source, and file name.

To view the FTP Get log:

1. Click **Logs > Log Query > FTP Get Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Sort by**, select a sort order.
4. Click **Show Log**. The **FTP Get Log** screen opens.
5. Click **Refresh** to update the screen.

FTP Put Log

The FTP Put log contains all FTP Put transaction information, which includes user ID, date, sender identification, and file name.

To view the FTP Put log:

1. Click **Logs > Log Query > FTP Put Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Sort by**, select a sort option.
4. Click **Show Log**. The **FTP Put Log** viewing screen opens.
5. Click **Refresh** to update the screen.

Performance Log

The performance log contains information about server performance. Each performance metric record contains:

- Date and time the metric was recorded
- IWSVA device that recorded the metric
- Metric name (one of: `HTTP Requests Processed, HTTP Responses Processed, Number of HTTP threads, HTTP CPU % Utilization)`
- Metric value

To view the performance log:

1. Open the IWSVA Web console and click **Logs > Log Query > Performance Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, Last 30 days) from the drop-down menu.

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Sort by**, select a sort order.
4. Click **Show Log**. The **Performance Log** viewing screen opens.
5. Click **Refresh** to update the screen.

Spyware/Grayware Log

The spyware/grayware log contains information about spyware/grayware detected by IWSVA, including the name of the spyware/grayware, date, action, category, scan type, file name affected, user ID of the client involved, and Web protocol.

To view the spyware/grayware log:

1. Click **Logs > Log Query > Spyware/Grayware Log** in the main menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Grayware**, select the spyware/grayware for which you want to view log entries. Click **Add** (or **Add All** for all grayware listed).

   To remove grayware from the right list box, click **Remove** (or **Remove All** for all viruses listed).
4. Under **Protocol**, select a Web protocol type for which you want to view logs.
5. Under the **Sort by** section, select a sort option (Grayware, Date, Action, Category, Scan Type, File Name, User ID, Protocol).
6. Click **Show Log**. The **Spyware/Grayware Log** viewing screen opens.
7. Click **Refresh** to update the display.

System Event Log

The system event log contains information about state changes or errors that occurred in the system. The following types of events are recorded:

- Active updates
- Product registration
- System maintenance
- ARM database connection status (if using ARM)

To view the system event logs:

1. Click **Logs > Log Query > System Event Log** in the main menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, or Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Level(s)**, select the event level(s) for which you want to view log entries. Click **Add** (or **Add All** for all grayware listed).

To remove an event level from the right list box, click **Remove** (or **Remove All** for all levels listed).

4. Under the **Sort by** section, select a sort option (Server, Date, Level, or Source).
5. Click **Show Log**. The **System Event Log** viewing screen opens.
6. Click **Refresh** to update the display.

URL Blocking Log

The URL Blocking log contains information about URLs that have been blocked including the date and time the blocking event occurred, category, blocking rule applied, user ID, Outbreak Prevention Policy (OPP) ID if applicable, and scan type.

To view the URL blocking log:

1. Click **Logs > Log Query > URL Blocking Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, or Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **URLs blocked**, you can add the URL(s) listed in the left list box to the right list box.

   Highlight the URL(s) to add, then click **Add** (or **Add All** for all URLs listed). To remove the list of URLs from the right list box, click **Remove** (or **Remove All** for all URLs listed).
4. Under **Protocol**, select a Web protocol type for which you want to view logs.
5. Under **Sort by**, select the appropriate option to sort the display log.
   - **URL**—The blocked URL
   - **Date**—The date and time when the URL was blocked
   - **Category**—The rule defined by the user in the URL filtering, Access Quota, file blocking, and URL blocking policy
   - **Rule**—How the URL was blocked:
     - **IWSVA-defined rule (block the URL containing a virus):** Displays the URL that has been blocked
     - **URL blocking rule:** Displays the URL in the block list
     - **URL filtering rule:** Displays the policy name
     - **OPP defined rule:** Displays the OPP rule

- **File type defined rule:** Displays blocked file type
- **Phish defined rule:** Displays a Phish violation rule
- **Access Quota defined rule:** Displays access quota violation rule

- **User ID**—The IP address, host name, or LDAP user/group name associated with the client that requested the URL
- **OPP ID**—The ID number of the Outbreak Prevention Policy (OPP)
- **Scan Type**—Either URL filter, URL block, or Phish trap
- **Protocol**—Type of Web connection (HTTPS, HTTP, or FTP)

6. Click **Show Log**. The **URL Blocking Log** viewing screen opens.
7. Click **Refresh** to update the screen.

Note: You can also find an entry in the **URL Blocking Log** when an FTP proxy blocks a file by type.

URL Filtering Log

The URL filtering log contains information on filtered URLs (those that are blocked or monitored) including the date and time the filtering action occurred, category, URL filtering rule applied, user ID, and scan type.

To view the URL filtering log:

1. Click **Logs > Log Query > URL Filtering Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, or Last 30 days).

   Click **Range** to select a time range, then select the start and end dates.
3. Under **URLs filtered**, you can add the URL(s) listed in the left list box to the right list box.

   Highlight the URL(s) to add, then click **Add** (or **Add All** for all URLs listed). To remove the list of URLs from the right list box, click **Remove** (or **Remove All** for all URLs listed).
4. Under **Protocol**, select a Web protocol type for which you want to view logs.
5. Select the filtering action (**Block, Monitor, Warn,** and/or **Warn and Continue**) for which you want to view logs.

6. Under **Sort by**, select the appropriate option to sort the display log.
   - **URL**—The filtered URL
   - **Date**—The date and time when the URL was filtered
   - **Category**—The rule defined by the user in the URL filtering policy
   - **Rule**—How the URL was filtered
     - **URL filtering rule:** Displays the policy name
   - **User ID**—The IP address, host name, or LDAP user/group name associated with the client that requested the URL
   - **Scan Type**—Content filter scan type
   - **Protocol**—Type of Web connection (HTTP or HTTPS)
   - **Filtering action**—The filtering action applied to a given URL or category
7. Click **Show Log**. The **URL Filtering Log** viewing screen opens.
8. Click **Refresh** to update the screen.

URL Access Log

The URL access log contains URL access information. IWSVA writes to the URL access log only when **Log HTTP/HTTPS/FTP access events** is enabled (**Log HTTP/HTTPS/FTP access events** is disabled by default) under **Logs > Log Settings > Reporting Logs**. Each access monitoring record contains the following information:

- Date and time the access occurred
- User who visited the site
- IWSVA device that processed the access
- IP address of the client system that requested the access

Note: Network address translation might render this data meaningless, or at least make it appear that all access occurs from a single client. Also, when the access log is enabled, the IWSVA service is restarted. During the restart, a router might take up to 30 seconds to recognize IWSVA again, during which time the router does not redirect packets.

- Domain accessed

- Path portion of the URL (the HTTP service can get the full URL path)
- IP address of the server from which the data was retrieved
- The URL category for every access event

To view the URL access log:

1. Open the IWSVA Web console and click **Logs > Log Query > URL Access Log** in the main menu.
2. Select a **Time period** (All Dates, Today, Last 7 days, or Last 30 days) from the drop-down menu.

   Click **Range** to select a time range, then select the start and end dates.
3. Under **Protocol**, select a Web protocol type for which you want to view logs.
4. Under **Sort by**, select a sort option.
5. Click **Show Log**. The **URL Access Log** viewing screen opens.
6. Click **Refresh** to update the URL access log.

Virus Log

The virus log contains information about viruses that IWSVA has detected.

To view the virus log:

1. Click **Logs > Log Query > Virus Log** in the main menu.
2. Under **Time period**, select the time for which you want a report generated.

   Click **Range** to view the virus log in a given time range, then select the start and end dates.
3. Under **Viruses**, select the virus(es) for which you want to view log entries. Click **Add** (or **Add All** for all viruses listed). To remove virus(es) from the right list box, click **Remove** (or **Remove All** for all viruses listed).
4. Under **Protocol**, select a Web protocol type for which you want to view logs.
5. Under the **Sort by** section, select an option by which to sort the display log.
6. Click **Show Log**. The **Virus Log** screen opens.
7. Click **Refresh** to update the screen.

Deleting Logs

If you no longer need to refer to text log files, you can delete them from the directory.

Note: The following procedure deletes text log files; logs in the database cannot be deleted manually. Configure a scheduled deletion for database logs on the **Logs > Log Settings** screen.

To delete one or more logs:

1. Click **Logs > Log Deletion** in the main menu.
2. On each of the four tabs (**Virus Log**, **URL Blocking Log**, **URL Access Log**, **Performance Log**, and **System Event Log**) select the log to delete.
3. Click **Delete**, then confirm by clicking **OK** on the next screen.

Log Settings

From the **Log Settings** screen, you can configure:

- Directories for reporting and system logs (for the text log files only)
- Whether to gather performance data or log HTTP/HTTPS/FTP access events, and the logging interval for each
- Database log update interval, and the number of days to keep logs in the database
- Whether to write logs to database and log files, to the database only, or to the log file only

Note: Text log files cannot be automatically deleted—they can be manually deleted on the **Logs > Log Deletion** screen. Database logs cannot be manually deleted—a deletion schedule can be configured on the **Logs > Log Settings** screen.

Log File Folder Locations

You can configure the folders for the reporting logs and the system logs. The default location is `/var/iwss/log`. A folder must exist on the IWSVA device and you must have the correct permission before the folder can be configured as the log file location. IWSVA checks after a folder path is entered, and an error message appears if the folder entered is not accessible.

Note: `/etc/iscan/log` is a symbolic link to `/var/iwss/log`.

To configure reporting log directories:

1. Click **Logs > Log Settings > Reporting Logs** from the main menu.
2. In the corresponding text boxes, type the folder locations for the log files.
3. Click **Save**.

To configure the system log directories:

1. Click **Logs > Log Settings > System Logs**.
2. In the corresponding text boxes, type the folder locations for the log files.
3. Click **Save**.

Other Log Options

There are some additional settings that control how IWSVA logs events. These can be configured on the **Log Settings** screen.

System Logs

On the **System Logs** tab, configure the number of days to retain system logs before automatically deleting them (default = five days).

Reporting Logs

On the **Reporting Logs** tab, you can configure IWSVA to gather performance data and log HTTPS/HTTP/FTP access events. If you enable these, configure the logging interval to record access events (from 1 to 9 minutes). Then, configure how to log these events:

- **Log user's visit along with all downloaded files and objects (verbose)**—This verbose logging option captures all information for the user's visit. It logs the initial connection to the site as well as all objects on the web pages downloaded. This option requires extensive disk space use and should only be enabled if your logging requirements need this type of extensive logging. Enabling this option can also reduce the performance of the system if fast disk drive subsystems are not available.
- **Log user's visit along with any downloaded files and objects that are above the size XXXX KB**—This logging option captures the user's visit, or connection, to the web site and all associated files or objects greater than the size specified. This option allows you to capture information about where each user has visited and allows you to reduce the amount of logging events collected by fine-tuning the size parameter. The larger the size parameter, the less detailed file and object information is collected from the downloaded pages. This option provides the best trade-off between performance, size of logs, and information collected.
- **Log files and objects downloaded that are at least XXXX KB**—This logging option only captures file and objects downloaded that are larger than the specified size parameter. This option allows you to eliminate the collection of user connection information to the web site and is used to log events for web site objects equal to or greater than the specified size. This option can dramatically lower the amount of disk space needed for logging and should be used only when large object logging is required without user connection information.

The default time period that logs are kept in the database is 30 days; customize this to reflect your specific environment's needs. In addition, set the time interval that the database is updated with new logs (default = 30 seconds).

Log File Naming Conventions

By default, log files are written to the `/etc/iscan/log` directory. IWSVA has a standard convention for naming log files. For instance, the convention for virus logs is:

```
virus.log.2010.07.04
```

which can be read as virus log for July 4, 2010

The naming conventions for each type of log are described in *Figure 12-1*.

TABLE 12-1. Log File Naming Conventions

LOG	FILE NAME
Virus Log	virus.log.yyyy.mm.dd
URL Blocking/URL Filtering	url_blocking.log.yyyy.mm.dd.0001
Performance Log	perf.log.yyyy.mm.dd
URL Access Log	access.log.yyyy.mm.dd.0001
FTP Log	ftp.log.yyyymmdd.0001
HTTP Log	http.log.yyyymmdd.0001
Mail Delivery Log	mail.log.yyyymmdd.0001
Update Log	update.log.yyyymmdd.0001
Scheduled Update Log	admin.log.yyyymmdd.0001
System Event Log	systemevent.log.yyyy.mm.dd
Temporary Control Manager Log	CM.yyyymmdd.0001
Java Applet Scanning Log	jscan.log.yyyymmdd.0001
Audit Log	audit.trail.log
Database Import Tool Log	log_to_db.log.yyyymmdd.0001
World Virus Tracking Center Log	logtowvts.log.yyyymmdd.0001
HA Agent Log	ha_agent.yyyy.mm.dd

Note: Deleting a log does not necessarily prevent the corresponding data from appearing in the IWSVA Web console. To prevent IWSVA from displaying data, you must remove the corresponding data from the appropriate database table.

TABLE 12-3. Major Database Tables for IWSVA Logging/Reporting

TABLE NAME	EXAMPLE COLUMNS
tb_url_usage	username, URL, path
tb_report_by	period, category, entity_type, entity_name
tb_violation	username, URL, file_name, action, blocked_by, category
tb_performance_value	server, date_field, metric_value, metric_id

Exporting Log and Report Data as CSV Files

When viewing your log query or a real-time report, IWSVA supports exporting log data to a CSV file in order to view and analyze the data in other applications. Click **Export to CSV** and then download the file from the IWSVA server.

The character format that IWSVA uses to save CSV files is configurable using the `csvcharformat` parameter under the [Common] section of the `intscan.ini` file. The default is UTF-8 format. Some versions of Microsoft Excel cannot display double-byte characters in UTF-8 text files. If your logs contain double-byte characters, Trend Micro recommends opening and saving the files as Unicode using Notepad before attempting to open the CSV file using Excel.

Exporting Report Data as PDF Files

In addition to the CSV export feature, IWSVA also allows you to export report data as PDF files that can be viewed using a PDF-reader application in any platform. Click **PDF** and follow the on-screen prompt to download the file from the IWSVA server.

Syslog Configuration

With syslog server support, IWSVA can send logs to external syslog servers. You can configure up to a maximum of four syslog servers and specify the type or priority level of the logs to send to each syslog server.

To configure a syslog server:

1. Click **Logs > Syslog Configuration** in the main menu.
2. Click **Add**.
3. For **Syslog Server Settings**:
   a. Select **Enable Syslog** to allow IWSVA to send logs to this syslog server

   b. Specify the **Server Name/IP Address**

   c. Specify the **UDP Port** (the default is 514)
4. Under **Save the Following Logs**, specify the logs to send. You can select to send events to the syslog server by either the log type or the syslog priority level.
   - Click **By log type** and select the type(s) of logs. Or,
   - Click **By syslog priority level** and select the level(s)
5. Click **Save**.

Introduction to Notifications

Notifications can be issued in response to scanning, blocking, alerting, and program update events. There are two types of notifications—administrator notifications and user notifications. described as follows:

- **Administrator notifications** provide information about HTTP(s) scanning, HTTP(s) file blocking, FTP blocked file types, FTP scanning, threshold alerts, restricted tunnel traffic, High Availability events, and Applets/ActiveX security events, as well as pattern file and scan engine updates. IWSVA sends administrator notifications through email to addresses that you configure in the **Email Settings** screen.

- **User notifications** provide information about HTTPS access errors, HTTPS certificate warnings, HTTP(s) scannings, HTTP(s) file blockings, FTP scannings, URL blockings, FTP blocked file types, High Availability events, and Applets/ActiveX scanning events. IWSVA presents user notifications in the client's browser or FTP client in lieu of the prohibited Web page or file that the client is trying to view or download.

The messages presented in both the administrator and user notifications are configurable and can include "tokens" or variables to customize notification messages with information about the event. In addition, user notification messages support HTML tags to customize the appearance of the message and provide links to other resources, such as security policy documents hosted on your intranet.

Email Notification Settings

IWSVA sends administrator notifications to email addresses that you specify. The administrator enters email settings when installing IWSVA and when running the setup program, but email settings can also be modified post-installation on the Web console's **Email Settings** screen.

To configure email settings for administrator notifications:

1. Click **Notifications** in the main menu.
2. In the **Notifications** screen, click **Send notification to**.
3. Type the email address to send notifications, the sender's email address, the SMTP server, the SMTP server port, and the time interval between checking the mail queue.
4. If your mail server requires ESMTP, enable **Use Extended Hello (EHLO)** for IWSVA to initialize SMTP sessions using the EHLO command.
5. Click **Save**.

Notification Tokens/Parameters

To make notifications more meaningful, IWSVA can use tokens (or variables) as information placeholders in a notification. When an event occurs, IWSVA dynamically substitutes the specific information in place of the variable, providing detailed information about that specific event.

For example, you could create a generic notification as follows:

```
A virus was detected in HTTP traffic.
```

This notification lets you know there is a problem, but does not provide any details. Instead, you could configure the notification using variables as follows:

```
On %Y, IWSVA detected a security risk %v in the file %F. %N
attempted to download the file from %U.
```

The notification might read as follows:

```
On 5/28/08 6:31:56 PM, IWSVA detected a security risk
JS_TEST_VIRUS in the file EXT_JS.JS. 10.2.203.130 attempted
to download the file from
http://10.2.203.130/TESTDATA/virus/NonCleanable/EXT_JS.JS
```

With this information, administrators can contact the client and provide more security information. The notification in this example uses five variables: %Y, %v, %F, %N and %U.

The following table contains a list of variables that can be used in notification messages and pages.

TABLE 12-4. Description of Variables

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
HTTPS Notifications		
%h	IWSVA hostname	The IWSVA host name where the event was triggered
%u	URL/URI	
%c	IP address:port after "https://"	Refer to the default message for %c usage example
$$DETAILS	Details of certificate failure reason / access denied reason	
HTTPS/HTTP and FTP Scanning		
%A	Action taken	The action taken by IWSVA

TABLE 12-4. Description of Variables (Continued)

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
%F	File name	The name of the file in which a risk is detected, for example, anti_virus_test_file.htm
%H	IWSVA host name	The IWSVA host name where the event was triggered
%L	Detailed file name and reason	
%M	Moved to location	The quarantine folder location where a file was moved
%N	User name	
%R	Transfer direction	
%U	URL/URI	
%V	Malware name (virus, Trojan, and so on)	The name of the risk detected
%X	Reasons/block type	
%Y	Date and time	The date and time of the triggering event
HTTP/HTTPS/FTP File Type Block		
%U	URL/URI	
The following tokens are only used in messages for administrators or in user notification messages:		
%F	File name	
%A	Action taken	
%H	IWSVA host name	
%R	Transfer direction	
%X	Reasons/block type	
%Y	Date and time	
%N	User name	

TABLE 12-4. Description of Variables (Continued)

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
%V	Virus or Trojan	
Applets and ActiveX Security		
%D	Protocol being scanned	
%H	IWSVA host name	
%N	User name	
%U	URL/URI	
%W	New certificate information	
%X	[reasons/block type]	
%Y	Date and time	
%Z	Policy name	
HA events		
%H	Host name	
%P	Peer name	
%R	Reason	
IM and IntelliTunnel Security		
%D	Protocol being scanned (HTTP or FTP)	
%H	IWSVA host name	
%N	User name	
%U	URL/URI	
%X	Reason (the localized name of the blocked protocol)	
%Y	Date and time	
%Z	Policy name	
URL Blocked by Access Control		

TABLE 12-4. Description of Variables (Continued)

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
%H	IWSVA host name (only works in header field)	
%U	URL/URI (only works in body)	
%X	Reason (only works in body)	
URL Blocked by URL Filtering		
%C	Category	
%H	IWSVA host name (only works in header field)	
%U	URL/URI	
URL Access Warning		
%A	Action	
%B	Warn and continue	
%C	Category	
%H	IWSVA host name (only works in header field)	
%U	URL/URI (only works in body)	

To customize URL Access Warning notifications, the message template must contain following form to display the "Continue" option:

```
<form id="warncontinue" method="post" action="%B/$$$IWSX_URL_ACTION$$$">
<INPUT type=hidden value="%A" name=data>
</form>
```

A button or hyperlink must be defined to submit the form about the customized notification that allows users to continue. Example:

```
<a href="javascript:void(0)"
onclick="document.getElementById('warncontinue').submit();
return false;">Continue to this website (not recommended)</a>
```

TABLE 12-4. Description of Variables (Continued)

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
Threshold Notification		
%m	Metric	
%t	Threshold value	

Configuring Notifications

To configure a notification, select the types of events that issue the notification and then edit the email and browser notification messages.

Using HTML Tags in User Notifications

You can use HTML to format user notification messages. While the HTML files can include reference links to external images or styles, IWSVA only supports uploading HTML files. Any additional files have to be uploaded separately to a Web server, and Trend Micro recommends using absolute links to help avoid broken links.

Configuring Applets and ActiveX Security Notification Settings

When IWSVA detects an attempt to download a Java Applet or ActiveX object that violates a security policy, the application sends an administrator a notification through email and a user notification message in the requesting client's browser.

To configure the Applets and ActiveX security notification settings:

1. Click **Notifications** in the main menu, then click **Applets and ActiveX Instrumentation**.
2. Under **Administrator Notification**, select **Send a message when a malicious Applet or ActiveX attempt is detected**.
3. If you do not want to use the default notification messages, highlight the default text and type your own version. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 12-38.
4. For the **User Notification Messages**:
   a. Select **Default** to display the default warning message.

b. Select **Customized** to display a custom message and either type or import the customized message's content.

- You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
- You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

5. Click **Save**.

Configuring FTP Blocked File Type Notifications

In addition to scanning FTP uploads and downloads, InterScan Web Security Virtual Appliance can block file types at the FTP gateway. To prevent performance issues, the FTP scanning module supports special configurations for compressed files and large files. Spyware and grayware scanning is also supported.

InterScan Web Security Virtual Appliance FTP scanning can be deployed into your environment in conjunction with another FTP proxy server or InterScan Web Security Virtual Appliance can act as its own FTP proxy. And to help ensure the security of the InterScan Web Security Virtual Appliance server, several security-related configurations are available to control access to the InterScan Web Security Virtual Appliance server and its ports.

To configure the FTP blocked file type notification settings:

1. Click **Notifications** on the main menu, then click **FTP Blocked File Type.**
2. Under **Administrator Notification**, check **Send a message when the FTP blocked file type is accessed.**

   Depending on what IWSVA is configured to block, this option can result in a large number of notification messages sent to the default recipient. As an alternative to item-by-item notifications, bear in mind that blocked files are written to a log, and can be included in one of the IWSVA generated reports.
3. If you do not want to use the default notification messages, highlight the default text and type your own. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 12-38.
4. For the **User Notification Message**:

   a. Select **Default** to display the default warning message.

   b. Select **Customized** to display a custom message and type the customized content.

      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

5. Click **Save**.

Configuring FTP Scanning Notification Settings

When IWSVA detects malicious code in a user's FTP transfer, it can automatically send a customized administrator notification to the designated email addresses and/or display a notification in the requesting FTP client program.

To configure the FTP scanning notification settings:

1. Click **Notifications** on the main menu, then click **FTP Scanning**.
2. Under **Administrator Notification**, select the trigger detection events for sending a notification (**Virus** and/or **Trojan** and/or **Other malicious code**).
3. If you do not want to use the default notification messages, highlight the default text and type your own. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 12-38.
4. For the **User Notification Message**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message and type the customized content.
      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
5. Click **Save**.

Configuring High Availability Events Notifications

Notifications can be configured for the following HA events:

- Switchover
- Child Server Failure
- Recovered Child Server
- Configuration Sync Failure

To configure HA event notifications:

1. Click **Notifications** on the main menu, then click **High Availability Events.**
2. Click the "**Send a message when...**" check box to have a message sent for the specific HA event. You may check one or more.
3. Use the default message or replace it with your own custom message for any or all of the four events notifications.
4. Click **Save**.

Configuring HTTP/HTTPS File Blocking Notifications

When IWSVA blocks a file, it sends an administrator notification through email, and a user notification message is displayed in the requesting client's browser.

To configure HTTP/HTTPS file blocking notifications:

1. Click **Notifications** and then click **HTTP/HTTPS Blocked File Type**.
2. Under **Administrator Notification**, select **Send a message when the blocked file type is accessed**.
3. If you do not want to use the default notification message, highlight the default text and type your own version. If applicable, insert tokens in the text as described in Notification Tokens/Parameters starting on page 12-38.
4. Type the **Headline** to appear in the browser.

   The default headline is *Trend Micro InterScan Web Security Event*. The headline is common for virus infection messages, file-type blocking, and URL blocking messages.
5. For the **User Notification Message**:
   a. Select **Default** to display the default warning message.

b. Select **Customized** to display a custom message and either type or import content from an HTML file.

- You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
- You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

6. Verify the notifications by clicking **Preview**.
7. Click **Save**.

Configure HTTP/HTTPS Scanning Notifications

When IWSVA detects malicious code in a file requested by a client, it issues an administrator notification through email and a user notification in the requesting client's browser.

Because IntelliTrap is considered a type of security threat, it uses the same notifications as HTTP/HTTPS Scanning.

To configure HTTP/HTTPS scanning notifications:

1. Click **Notifications** and then click **HTTP/HTTPS Scanning**.
2. Under **Administrator Notification**, select the trigger detection events for sending a notification (**Virus** and/or **Trojan** and/or **Other Internet Threats.**)

Note: IntelliTrap notification is associated with **Other Internet Threats**. Therefore, IntelliTrap notification is enabled when you select **Other Internet Threats**.

3. If you do not want to use the default notification message, highlight the default text and type your own version. If applicable, insert tokens in the message as described in Notification Tokens/Parameters starting on page 12-38.
4. Type the **Headline** to appear in the browser.

   The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.
5. For the **User Notification Message** for **Message for downloaded file** and **Message for uploaded file**:

a. Select **Default** to display the default warning message.

b. Select **Customized** to display a custom message and either type or import the customized message's content from an HTML file.

- You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
- You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

c. Verify that the notifications appear correctly by clicking **Preview**.

6. Click **Save**.

Configuring HTTPS Access Denied Notifications

Whenever users are denied to access a Web site through HTTPS connections, they will see an HTML page explaining that their request has been rejected.

To configure HTTPS access denied notifications:

1. Click **Notifications** and then click **HTTPS Access Denied**.
2. Type the **Headline** to appear in the browser.

   The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.
3. For the **User Notification Message**:

   a. Select **Default** to display the default warning message.

   b. Select **Customized** to display a custom message and either type or import content from an HTML file.

   - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
   - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
4. Verify the notifications by clicking **Preview**.
5. Click **Save**.

Configuring HTTPS Certificate Failure Notifications

Whenever users are denied to access a Web site whose certificate does not pass the verification tests, they will see an HTML screen with the warning message. Users have the option to continue accessing the Web site without decrypting and checking HTTPS traffic.

To configure HTTPS certificate failure notifications:

1. Click **Notifications** and then click **HTTPS Certificate Failure**.
2. Type the **Headline** to appear in the browser.

   The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.
3. For the **User Notification Message**:
   - **a.** Select **Default** to display the default warning message.
   - **b.** Select **Customized** to display a custom message and either type or import content from an HTML file.
     - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
     - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
4. Verify the notifications by clicking **Preview**.
5. Click **Save**.

Configuring IntelliTunnel Security Notification Settings

When IWSVA detects restricted tunnel traffic across port 80, the application blocks this traffic and sends an email to the address specified on the IntelliTunnel Notification page. See IntelliTunnel Security on page 7-44.

To configure the IntelliTunnel security notification settings:

1. Click **Notifications** in the main menu, then click **IntelliTunnel**.
2. Under **Administrator Notification**, select **Send a message when restricted tunnel traffic is detected**.

3. If you do not want to use the default notification messages, highlight the default text and type your own version. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 12-38
4. Click **Save**.

Enabling Pattern File Update Notifications

IWSVA can send notifications when the product attempts to update engines or pattern files based on scheduled pattern updates.

Note: IWSVA will not send notifications for manual pattern updates.

To enable pattern file update notifications:

1. Click **Notifications** from the main menu, then click **Pattern File Updates**.
2. For the pattern update attempts:
   a. Select the update events that trigger a notification. You can configure notifications for **Successful**, **Unsuccessful** or **Not needed** update attempts.

   b. Type a **Subject** for the notification message. Default is *IWSVA pattern update result*.
3. Click **Save**.

Enabling Threshold Alerts Notifications

You can specify threshold alert values and the frequency of alerts so that you are notified when the level of any of the following items reaches a critical level:

- Virus
- Spyware
- Database
- Hard drive
- Bandwidth

IWSVA can send these alerts either through email, SNMP trap/notification (if enabled), or both. See *Email Notification Settings* on page 12-38.

Note: Configure threshold alert settings for email notifications. Threshold alert settings do not affect when IWSVA sends SNMP traps.

To enable threshold alert notifications:

1. Click **Notifications** in the main menu, then click **Threshold Alerts**.
2. Under **Thresholds**, specify the desired thresholds and either accept the defaults or specify new values in the **Threshold Value** and **Limit 1 Notification Every** columns.
3. If you do not want to use the default notification messages under **Notification Message**, highlight the default text and type your own version. If applicable, insert variables in the text as described in Notification Tokens/Parameters starting on page 12-38.
4. Click **Save**.

Configuring a URL Blocking by Access Control Notifications

When IWSVA detects an attempt to access a URL in the Phish pattern file or a prohibited URL from the local IWSVA list, IWSVA displays a warning screen in the browser of the requesting client to indicate the URL was blocked.

To configure a user notification message for URL Blocking by Access Control:

1. Click **Notifications** in the main menu, then click **URL Blocking by Access Control**.
2. Under **User Notification Message for Restricted or Blocked URLs**:
   a. Type the **Headline** to appear in the browser.

      The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.

   b. Click **Default** to display the default warning message.

   c. Click **Customized** to display your own warning message. Type the message in the text box, or **Import** it from a HTML file on your local machine.

      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).

- You can append a custom message to the IWSVA default by selecting both the Default and Customized options.

3. Verify the notifications by clicking **Preview**.
4. Click **Save**.

Configuring a URL Blocking by URL Filtering Notifications

When IWSVA detects an attempt to access a URL in the Phish pattern file or a prohibited URL from the local IWSVA list, IWSVA displays a warning screen in the browser of the requesting client to indicate the URL was blocked.

To configure a user notification message for URL Blocking by URL Filtering:

1. Click **Notifications** in the main menu, then click **URL Blocking by URL Filtering**.
2. Under **User Notification Message for Restricted or Blocked URLs**:
   a. Type the **Headline** to appear in the browser.

      The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection, file-type blocking, and URL blocking messages.

   b. Click **Default** to display the default warning message.

   c. Click **Customized** to display your own warning message. Type the message in the text box, or **Import** it from a HTML file on your local machine.

      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
3. Verify the notifications by clicking **Preview**.
4. Click **Save**.

Enabling Notifications for URL Filtering Engine and Scan Engine Updates

Though less frequent than pattern file updates, Trend Micro periodically releases new versions of the scan engine to reflect advances in virus and malicious code detection methods. IWSVA can issue administrator notifications in response to scheduled scan engine updates.

Note: IWSVA will not send notifications for manual engine updates.

To enable URL Filtering and Scan Engines Update Notifications:

1. Click **Notifications** from the main menu, then click **URL Filtering and Scan Engines Update**.
2. For the scan engine and/or the URL filtering engine, select the update events to trigger a notification.

   You can configure notifications for **Successful**, **Unsuccessful,** or **Not needed** update attempts.
3. For the scan engine and/or the URL filtering engine, type the **Subject** of the notification email message.
4. Click **Save**.

Configuring URL Access Warning Notifications

The URL Access Warning Mode sends notifications if the URL Filtering rules action is set to “Warn” and the user attempts to access a URL that belongs to a category prohibited by company policy. (See Creating a New Policy on page 9-5 for details.) The user receives the warning before seeing the Web page.

The user has an option to click one of the following links in the warning message:

- Click here to exit this Web page and go back to the previous page OR
- Continue to this Web site (not recommended)

To configure the URL Access Warning notifications:

1. Click **Notifications** on the main menu and then click **URL Access Warning**.
2. Type the **Headline** to appear in the browser.

The default is *Trend Micro InterScan Web Security Event*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.

3. For the **User Notification Message**:
   a. Select **Default** to display the default warning message.
   b. Select **Customized** to display a custom message and either type or import content from an HTML file.
      - You can design your own notification page using any HTML editor, then **Import** the page to IWSVA (for example, if you want to display company brandings, or provide a link to additional resources).
      - You can append a custom message to the IWSVA default by selecting both the Default and Customized options.
      - The notification must contain a form to submit necessary information to IWSVA if end users choose to continue. The format is:

```
<form id="warncontinue" method="post" action="%B/$$$IWSX_URL_ACTION$$$">

<INPUT type=hidden value="%A" name=data>

</form>
```

      - A button or hyperlink must be defined to submit the form about the customized notification for users to continue. Example:

```
<a href="javascript:void(0)"
onclick="document.getElementById('warncontinue').submit();

return false;">Continue to this website (not recommended)</a>
```

4. Verify the notifications by clicking **Preview**.
5. Click **Save**.

Enabling SNMP Trap Notifications

IWSVA supports sending SNMP traps in response to security, update, or program events.

Note: To send SNMP traps, you first need to configure the SNMP settings and then enable this feature. To do this, choose **Administration > Network Configuration > SNMP Settings**.

To enable sending SNMP traps:

1. Click **Notifications** on the main menu and then click **SNMP Notification Settings. . .** at the bottom of the screen.
2. Select the types of events that triggers an SNMP trap. The different classes of events are:
   - **Virus or Internet threats**—Events related to virus or malicious code detections
   - **Security violations**—Activities that are prohibited by IWSVA policies, not related to viruses or malicious code
   - **Pattern, database or scan engine updates**—Events related to IWSVA updates
   - **IWSVA service interruptions**—Issues with any of the essential IWSVA services
   - **System performance metric**—IWSVA periodically sends an SNMP trap with the following performance data:
     - CPU load percentage
     - Memory load percentage
     - Disk load percentage
     - Concurrent connection (ICAP request and response mode and proxy mode)
     - Incoming and outgoing throughput (bytes per second)
   - **High Availability events**—Issues with any of the essential HA functions, if HA is used.
   - **Hardware monitoring events**—Events related to monitored hardware components:
     - Voltage
     - Fan
     - CPU
     - Storage
     - Temperature
3. Click **Save**.

Enabling MAC Address Client Identification

If you select Host name (modified HTTP headers) in the User Identification screen, IWSVA displays client IP address information in logs, reports, and notifications. You can also configure IWSVA to display client MAC address information.

Note: To identify a client by the MAC address, you must select **Host name (modified HTTP headers)** in the User Identification screen. Host name identification is only supported for end-users browsing with Internet Explorer on Microsoft Windows platforms.

To display client MAC addresses in logs, notifications, and reports:

1. You can obtain the `register_user_agent_header.exe` file from the `/usr/iwss/bin` folder on the IWSVA server or download it from following Web site:

   `http://www.trendmicro.com/download/product.asp?productid=86`

2. Run `register_user_agent_header.exe` on each client computer. The program configures the computer to include MAC address information in data packets.
3. Log on to the Web console on the IWSVA server and make sure the **Host name (modified HTTP headers)** option is selected in the User Identification screen (**HTTP > Configuration > User Identification | User Identification).**
4. Access the privileged CLI commands on the IWSVA server and type: `configure module identification mac_address enable`.

To disable client MAC address identification:

Access the privileged commands on the IWSVA server and type: `configure module identification mac_address disable`.

Advanced Reporting and Management (ARM) Integration

This section focuses on IWSVA's integration with Trend Micro Advanced Reporting and Management (ARM), including registering and unregistering, and the IWSVA features affected by ARM registration.

Topics include:

- Introducing ARM on page 12-57
- ARM Registration and Unregistration on page 12-58
- Feature Changes after ARM Registration on page 12-58

Introducing ARM

Trend Micro Advanced Reporting and Management (ARM) provides customers with a high-performance, off-box reporting solution. ARM is based on new advanced database technology that greatly enhances the current InterScan Web Security product reporting capabilities and provides advanced features, such as dynamic dashboard, drill-down reporting, custom reporting, and real-time, problem-solving capabilities.

ARM provides a centralized reporting and policy management solution that includes:

- Instant reporting capabilities for IWSVA pre-canned report types to eliminate or reduce reports that take many hours to complete
- Centralized logging and reporting for multiple InterScan Web Security product units
- Custom reporting with GUI interface for fast report creation, using iReport
- Real-time, historic, and ad hoc reporting capabilities
- Dynamic dashboard for true Network Operation Center (NOC) monitoring
- Ability to troubleshoot with drill down reporting
- Central policy management and synchronization between multiple managed InterScan Web Security product units

ARM Registration and Unregistration

IWSVA can register to ARM as a standalone device, or as a cluster member if the device is configured to belong to a HA cluster before registering to ARM. When IWSVA registers to ARM as a HA cluster member, it will share the parent member's IWSVA policies. See Chapter 3, High Availability and Cluster Management on page 3-1 for details.

IWSVA registration is initialized from the ARM server using the Device Registration function. After registration, IWSVA will use ARM's remote database for all logging and reporting functions. However, policy databases will remain locally on the IWSVA device to allow the IWSVA to continue functioning in the event of a bad network connection between the IWSVA and ARM devices. If the connection between the IWSVA and ARM devices is down or the ARM device is non-functional, logging and reporting functions will not be possible as IWSVA cannot send its event information to ARM for processing. In the case where the ARM device is not reachable for long periods of time, you may want to un-register the IWSVA devices from ARM to allow IWSVA to perform local logging and reporting functions.

Normally, IWSVA un-registration is also initiated from the ARM server using the Device Registration function if the connection between IWSVA and ARM is functioning properly. However if the connection between the IWSVA and ARM devices is broken (in the case of a bad network connection), the un-registration process can be initiated manually from the IWSVA device using the following CLI command: `configure module arm disable`. If you manually un-register IWSVA from ARM, all logging and reporting functions will be reverted back to the IWSVA's local databases.

But since the ARM device was down or the connection was broken, you must remember to also un-register the IWSVA devices from the ARM server using the Device Registration function when ARM becomes available. This allows ARM and IWSVA to stay in synch when the connection is restored between the two devices.

For more information on the ARM register and unregister procedures, refer to the *Advanced Reporting and Management for InterScan Web Security Administrator's Guide*.

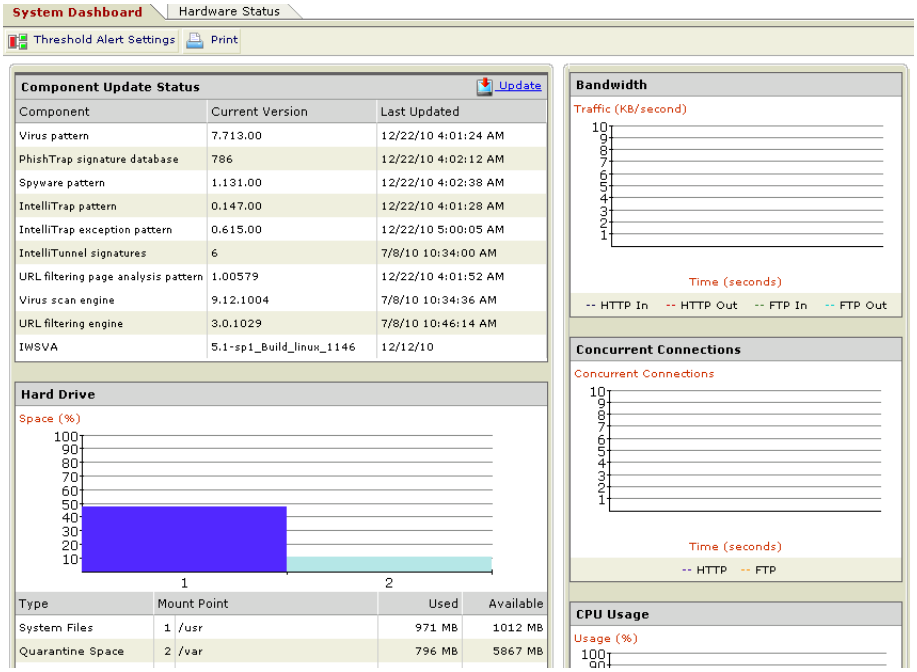
Feature Changes after ARM Registration

Because ARM provides enhanced reporting and log management capabilities, the following IWSVA features and Web screens are affected after ARM registration:

- Summary screen
- Logs and reports
- Notifications
- Command Line Interface (CLI)

Summary Screen

- All statistic tabs, including “Scanning,” “URL,” “Spyware,” and “Security Risk Report” do not display in the Summary screen.
- In the System Dashboard, the following are removed:
    - Virus and Spyware Trend table
    - All 1day/30 days statistics for “Bandwidth,” “CPU Usage,” and “Physical Memory Usage”



Component Update Status

Component	Current Version	Last Updated
Virus pattern	7.713.00	12/22/10 4:01:24 AM
PhishTrap signature database	786	12/22/10 4:02:12 AM
Spyware pattern	1.131.00	12/22/10 4:02:38 AM
IntelliTrap pattern	0.147.00	12/22/10 4:01:28 AM
IntelliTrap exception pattern	0.615.00	12/22/10 5:00:05 AM
IntelliTunnel signatures	6	7/8/10 10:34:00 AM
URL filtering page analysis pattern	1.00579	12/22/10 4:01:52 AM
Virus scan engine	9.12.1004	7/8/10 10:34:36 AM
URL filtering engine	3.0.1029	7/8/10 10:46:14 AM
IWSVA	5.1-sp1_Build_linux_1146	12/12/10

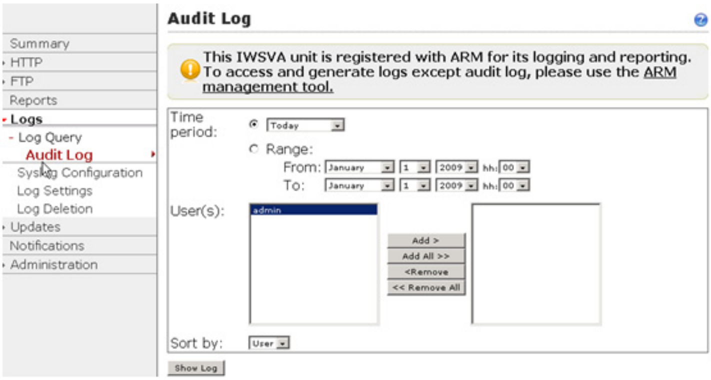
Type	Mount Point	Used	Available
System Files	1 /usr	971 MB	1012 MB
Quarantine Space	2 /var	796 MB	5867 MB

FIGURE 12-2. Summary screen changes after ARM registration

Logs and Reports

After IWSVA is registered to ARM, IWSVA automatically connects to and sends log data to the ARM database. The following log query and reporting functions are modified:

- **Log query**—Log queries (except for audit log) are disabled on IWSVA and the respective Web console screens do not display. A message displays in the IWSVA Web console to direct you to view related log information using the ARM management tool. You can click the link to access the ARM Web console. *Figure 12-3* shows an example.



Audit Log

This IWSVA unit is registered with ARM for its logging and reporting. To access and generate logs except audit log, please use the ARM management tool.

Time period: ● Today ○ Range: From: January 1 2009 hh: 00 To: January 1 2009 hh: 00

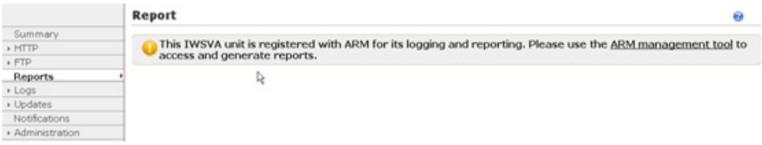
User(s): admin

Sort by: User

FIGURE 12-3. Log query function changes after ARM registration

- **Log settings**—Because IWSVA sends log data to the ARM database, settings to the local database IWSVA uses are no longer relevant. Thus, the following local database settings are disabled:
    - Number of days to store logs in database
    - “Text only” option for the Write logs setting

- **Reports**—All report screens are disabled in the IWSVA Web console. A message displays prompting you to access the ARM management tool to view generated reports.



Report

This IWSVA unit is registered with ARM for its logging and reporting. Please use the ARM management tool to access and generate reports.

FIGURE 12-4. Reports function changes after ARM registration

- **Notification**—In the IWSVA Web console, the threshold alerts setting for local database is disabled.
- **Command Line Interface (CLI)**— In previous versions of IWSVA, if IWSVA was registered to ARM, the database-related commands were disabled in the CLI. Now database-related commands are enabled in the CLI and operate only the local database, which is the policy database.

Chapter 13

Administration

This chapter describes the administrative functions available in IWSVA.

Topics in this chapter include the following:

Overview

The Administration menu includes the following options:

- IWSVA Configuration on page 13-2
  - Cluster Management on page 13-3
  - Policy Deployment on page 13-3
  - Database Connection on page 13-4
  - Quarantine Management on page 13-4
  - System Time on page 13-6
  - Register to Control Manger on page 13-6
  - Damage Cleanup Services Registration on page 13-7
- Network Configuration on page 13-8
  - Web Console on page 13-8
  - Remote CLI on page 13-9
  - SNMP Settings on page 13-9
  - Static Routes on page 13-10
- Management Console on page 13-11
  - Account Administration on page 13-12
  - Management Access Control on page 13-12
- Config Backup/Restore on page 13-14
- System Updates on page 13-14
- System Maintenance on page 13-15
- Product License on page 13-16
- Support on page 13-19

IWSVA Configuration

IWSVA Configuration contains the following items:

- Cluster Management on page 13-3
- Policy Deployment on page 13-3
- Database Connection on page 13-4

- System Time on page 13-6
- Register to Control Manger on page 13-6
- Damage Cleanup Services Registration on page 13-7

Cluster Management

The Cluster Management page allows users to view cluster settings, access to modifying cluster settings, and quick login access to child servers.

Click the Modify link to access the cluster settings modification page.

Go the Summary page of the parent node and click **Synchronize Now** to synchronize the parent policy settings to the child node.

Note: You can restrict contact with the parent to only those servers appearing on an approved list. The child member of the cluster will inherit the parent's approved list after synchronization. Contact requests from any machine not on the list will be rejected.

For more information on setting up and managing clusters, see the following sections:

- Create a New Cluster on page 2-6
- Join an Existing Cluster on page 2-7
- About Cluster Management on page 3-10
- Synchronizing Nodes Manually on page 3-7
- Deleting a Child Member from a Cluster on page 3-16
- Dissolving a Cluster on page 3-16
- Performing a Manual Switchover on page 3-17
- Modifying a Cluster on page 3-17

Policy Deployment

After creating or modifying a policy, you can immediately deploy it to the IWSVA policy database by clicking **Deploy**. Alternatively, you can do nothing and the policies will be automatically deployed according to the Time-to-Live (TTL) interval set in the Administration > Policy Deployment page.

By default, IWSVA will automatically deploy new policies after 30 minutes for the following types of policies:

- Virus scan
- HTTPS
- Applet and ActiveX
- IntelliTunnel
- URL filtering
- Access quota

Database Connection

IWSVA uses either an existing PostgreSQL database, or installs its own PostgreSQL database. The database holds policy settings and log data. Product configuration settings are stored in the "intscan.ini" file. These fields show the choices made during Setup, and should not be changed independent of the Linux ODBC Data Source.

Database Connection Settings:

- **ODBC data source name**—Shows the ODBC name chosen during Setup.
- **User name**—Shows the user name for the ODBC data source; determined during Setup. Default is "sa"
- **Password**—Displays the encrypted ODBC password chosen during Setup.
- **Test Database Connection**—Click to check that the Policy Database and Log Database connections are correct and that the connection is working. Response messages are generated from the native ODBC data source.

Quarantine Management

Most Internet threats, including spyware, Trojans, and worms cannot be "cleaned" because they do not actually "infect" the file. Trend Micro recommends you delete worms (because of the huge numbers possible) and quarantine or delete spyware, Trojans, and other unwanted programs that IWSVA has been configured to detect.

Quarantine Directory

Specify quarantine directory—When the Scan Policy Action for HTTP and/or FTP scanning is Quarantine, IWSVA moves those files to the directory specified here. The default location is:

```
/var/iwss/quarantine
```

Note: Trend Micro recommends that you encrypt all quarantined files as described inEncrypting Quarantined Files on page 13-5.

Encrypting Quarantined Files

Quarantined files are likely to be dangerous. Encrypting files for quarantine can help protect against accidental reinfection or the effects of some other type of malicious code.

Trend Micro recommends that if you choose to quarantine rather than delete suspect files, that you encrypt them before saving to the quarantine directory.

Note: See the "How to" section of the IWSVA Online Help for instructions on decrypting quarantined files.

To encrypt HTTP quarantines:

1. Click **HTTP > HTTP Scan > Policie**s, and then either choose an existing policy from the list, or click **Add** to create a new one.
2. Open the Virus Scan Rule tab. At the bottom of the page, click the **Encrypt quarantined files** check box.

To encrypt FTP quarantines:

1. Click **FTP > Scan Rules**.
2. Open the Virus Scan Rule tab. At the bottom of the page, click **Encrypt quarantined files**.

System Time

In the System Time page if the IWSVA Web console, you can manually configure the date and time. IWSVA also supports NTP servers and synchronizes the date and time information based on the specified schedule.

System Time Settings

Synchronize date and time with an NTP server—Select this option to obtain date and time information from the specified NTP server. You can enable automatic time synchronization based on the schedule you select from the list. Click **Synchronize Now** to connect to the NTP server and update the system date and time. This also allows you to test whether the NTP server is available.

Set the system time manually—Select this option and enter the system date and time in the fields.

Time Zone

Select your continent and nearest city from the lists provided.

Register to Control Manger

Use the **Administration > IWSVA Configuration > Register to Control Manager** screen to configure the communication between the localhost.localdomain Management and Communication Protocol (MCP) Agent and Trend Micro Control Manager server.

- **Connection Settings**—Specify the entity name (instance of IWSVA on the particular machine). The entity name appears in the Control Manager product tree, helping you to identify the product.
- **Control Manager Server Settings**—Specify the FQDN (Fully Qualified Domain Name) or IP address of the Control Manager server. The Web server authentication user name is used by the Internet Information Services (IIS) server for authentication. This information is not used by Control Manager.
- **MCP Proxy Settings**—In this section, specify the proxy server for communication with the Control Manager server.

- **Two Way Communication Port Forwarding**—Two-way communication allows the TMCM server to send commands in real-time to IWSVA. If the user does not specify this information, the agent defaults to one-way communication, which means IWSVA polls the TMCM server at set intervals to retrieve the commands.

Damage Cleanup Services Registration

If you have one or more Trend Micro Damage Cleanup Service (DCS) installed on the network, you can have IWSVA work in conjunction with them.

This is an especially useful relationship on networks where client laptops or visitors join the LAN. If the client already contains a Trojan, spyware, worm, or attempts to access known phish sites or disease vectors, IWSVA can detect and block the spurious outbound HTTP activity. It will also request the DCS server to conduct a clean up of the affected machine(s).

- **Enable DCS**—Select this option to engage the relationship between IWSVA and DCS. If IWSVA detects suspicious activity, it blocks the outbound access and sends the client's IP address to the DCS server for clean up. DCS also sends clean up logs to IWSVA when this option is enabled.
- **DCS server name or IP address**—Specify the IP address of the Damage Cleanup Server(s) you want to register.
  - To remove, or unregister a DCS server from IWSVA, click the trash bin icon next to the server from which you want to disconnect.
- **Port number**—The default HTTP port for the DCS server is 80. DCS does not support HTTPS.
- **Redirect client to DCS on cleanup failure**—Choose this option to have IWSVA redirect client HTTP requests to a "manual" DCS cleanup Web page if the DCS server could not clean the client.

  IWSVA only redirects the client if the DCS server reports that it was either unable to contact the client, or unable perform an automatic clean up on the client.

  If the client chooses not to perform a manual DCS clean up, and the browser does not support ActiveX, or if ActiveX is disabled, the client can navigate off the page and use the Internet as usual. After four hours (default), the client will again be directed to the manual DCS cleanup page.

  Default redirect time can be set in the file

```
/etc/iscan/intscan.ini
```

under the "infected_url_block_length" parameter.

Note: If you are using an HTTPS connection for the IWSVA console, see "Redirect Clients to DCS When IWSVA is using HTTPS" topic in the IWSVA product online help for important configuration steps.

You can view the logs sent by DCS from the IWSVA console, as well as the spyware detection reports

Network Configuration

Network Configuration includes the following items:

- Web Console on page 13-8
- Remote CLI on page 13-9
- SNMP Settings on page 13-9
- Static Routes on page 13-10

Web Console

By default, the IWSVA console is accessed through an HTTP connection on port 1812. For improved security, Trend Micro recommends that you use a Secure Socket Layer connection (HTTPS).

In bridge mode, IWSVA uses the ports specified as follows:

- **Non-SSL mode**—default; access the IWSVA console using a non-secure URL, for example:

  ```
  http://<IWSVA Server IP address:port>
  ```

  - **Port number**—default is 1812; can be changed to any unused port (recognized by the firewall)
- **SSL mode**—recommended; choose this option to enable a secure connection to the IWSVA console

- **SSL Certificate**—to support SSL, IWSVA needs a public key and certificate; locate the certificate you will use, and upload it to the IWSVA server
- **SSL Password**—enter the password associated with the SSL certificate, if any.
- **Port number**—enter the port on which you want to open the IWSVA console, for example:

  ```
  https://<IWSVA Server IP address:port>
  ```

Remote CLI

SSH (Secure Shell) is a network protocol that allows two network devices to exchange data in a secured connection. SSH replaces Telnet which sends data (including passwords) in clear text. IWSVA allows administrators to access the CLI from a remote location using SSH only.

Use **Administration > Network Configuration > Remote CLI** screen to configure SSH on IWSVA for remote CLI access.

- **SSH: Command line access**—Select this option to enable SSH connection for remote CLI access. Clear this check box to disable SSH service.
- **Port Number**—Type the service port number for SSH. The default port number is 22.

SNMP Settings

SNMP trap notifications are especially useful for monitoring the state of the IWSVA services—IWSVA issues a trap notifying you if a service stops unexpectedly. IWSVA supports SNMP agent notifications for the following events:

- HTTP, FTP, and ICAP service interruptions
- Virus pattern file, Tunnel pattern file, scan engine, and URL Filtering engine updates
- Security events
- HA events

Note: If IWSVA detects that the HTTP or FTP scanning service is down, it will try twice to restart it. If the service cannot be restarted, SNMP traps will be issued to the specified destination every 30 minutes until the service restarts.

System Information Setup

Specify all the necessary system information in the System Information section of the **Administration > Network Configuration > SNMP Settings** screen.

The community that you specify in the Community Name and Default Community fields identifies the community in which the SNMP object belongs. In SNMP, every managed object belongs to a community. This provides a minimal amount of security, because designating communities can define which SNMP agents can communicate.

Access Control Setup

Specify all the necessary access control information in the Access Control section of the **Administration > Network Configuration > SNMP Settings** screen.

The fields in this section are read-only because IWSVA sends simple status and alert messages. For the Read-Only Object Identifier (OID) field, the object ID (OID) is the code for a particular message, alert, or alarm. The "object" is the actual message, alert, or alarm.

Static Routes

Configure and deploy static route settings at **Administration > Network Configuration > Static Routes**.

Note: Static routes can also be added during deployment and changed using the **Administration > Deployment Wizard**.

The following provides a brief description of the options in this screen:

Add—Opens the Static Routes screen that allows you to create a new static route. You can add up to 50 static routes.

- If you bind a static route to an interface, the router setting must be in the same network segment as the interface.
- If you bind a static route to a port, the router setting must be in the same network segment as the port.

Delete—Deletes a static route from the list.

Network ID—Click a Network ID to edit settings.

Netmask—Displays the subnet mask of the router for this route.

Router—Displays the IP address of the router for this route.

Interface—Displays the interface that binds to this route.

Deployment Status—Displays whether a static route is deployed successfully.

Click **Deploy** after specifying all the required settings.

Configuring Static Routes

To configure a static route:

Enter the following:

- **Network ID**—Type the destination network or host ID.
- **Netmask**—Type the subnet mask.
- **Router**—Type the IP address of the router (the next hope) for this route.
- **Interface**—Select the interface that binds to this route. The router setting must be in the same network segment as the binding interface.

Management Console

The Management Console offers the following options:

- Account Administration on page 13-12
- Management Access Control on page 13-12

Account Administration

Account administration allows you to add and delete login accounts. It shows all the existing accounts, giving the username, a description, and the access rights, which are:

Administrator—Administrators have complete and unrestricted access to the system.

Auditor—Auditors cannot make any configuration changes. Auditors can only view configuration, generate real-time reports and view other reports.

Reports Only—Reports only can generate and view other reports.

Login Accounts

The Login Accounts page shows all the available login accounts.

- Click Add to create a new login account or click a username to edit an existing one.
- To delete a login account, select the check box associated with the login account and then click **Delete**.
- **Username**—The name of the user assigned to the login account.
- **Description**—The field that briefly describes the login account.
- **Access Rights**—There are three levels of access:
  - **Administrator**—Users have complete and unrestricted access to the system. They can read and modify any settings accessible through the console including creating, deleting, and modifying user accounts. Users with Administrator rights can log into IWSVA through an SSH connection. This is the default access for new users.
  - **Auditor**—Users cannot make any configuration changes; they can view configurations, logs, and reports and can also change their own passwords.
  - **Reports only**—Users can only view the Summary pages and scheduled reports. They can generate logs and real-time report queries and change their own passwords.

Management Access Control

An administrator can set the access control list (ACL) to restrict access to the management console (such as the Web console, CLI, and PING requests) or to a specific IP address or IP address range.

The management ACL is disabled by default, which allows any user to access the IWSVA management console. Administrators can add one or multiple IP addresses to the management ACL. Any IP address added to the management ACL can also be deleted individually. If the list is enabled, the administrator can only connect to the IWSVA management console from an IP address displayed on the allowed IP address list.

Note: Add the IP addresses of the central managers to which IWSVA registers (such as Trend Micro Control Manager, Advanced Reporting and Management, and so on) to the access list to allow them to function properly and access the necessary data from IWSVA.

To enable and configure the access control list for the management console:

1. Go to **Administration > Management Console > Management Access Control**.
2. Select one of the following options:
   - **IP address** - to add a single IP address to the management ACL
   - **IP range** - to add a range of IP addresses to the management ACL
   - **IP range netmask** - to add all the IP address covered by a network segment to the management ACL

   Note: No more than 20 entries can be added to the management ACL.

3. Click **Add** to add your entry to the allowed list.
4. Check the **Enable Administrative Access Based on Client IP** check box.

   Note: At least one IP address must be added to the management ACL before enabling this feature. Only users from the allowed IP address list can access the management console.

5. Click **Save**.
6. To delete an entry, click the **Delete** icon on the row of the entry to be deleted and confirm the deletion by clicking **Save**.

Config Backup/Restore

The Configuration Backup & Restore page is where you can generate an IWSVA configuration file for backup. Also from this page, the configuration and policy information for the following Trend Micro products can be migrated to IWSVA 5.1 SP1:

- IWSS 3.1 (Windows)
- IWSVA 5.1
- IWSVA 5.1 SP1

Note: For those using versions IWSVA 3.1 or IWSVA 5.0, you must upgrade to IWSVA 5.1 and then apply the IWSVA 5.1 SP1 patch.

IWSVA supports both full and partial migration. Use full migration to restore system and application settings or to apply current configuration to an IWSVA replacement machine. Perform a partial migration if you want to replace policy- and application-level configurations.

Note: 1. To perform a full migration, make sure the deployment mode, IP address, and network card(s) are the same on the two IWSVA machines.
2. OS settings, system patch information, and pattern files will not be updated after a full or partial migration.
3. IWSVA in High Availability mode only supports partial migration.

System Updates

From time to time, Trend Micro makes system updates available through the Download Center at: http://downloadcenter.trendmicro.com/

There are two kinds of system updates:

- Application patches
- OS updates

Both are handled in the same way and can be viewed in the History section of the Administration > System Updates screen. Only properly formatted and encrypted Trend Micro updates can be uploaded using this utility

To install a system update:

1. Get the latest update from the Trend Micro Download Center at: `http://downloadcenter.trendmicro.com/`
2. Go to **Administration > System Updates.**
3. Click **Browse** to locate the downloaded file.
4. Click **Upload**.
5. In the summary screen, click **Install**.
6. You may navigate to another screen after you receive the successful installation message.

Note: See Adding System Updates or Removing an Application Patch on page 14-19 for instructions on removing an application patch.

WARNING! **Updates available from other sources should never be applied to the IWSVA server.**

Note: After updating, the IWSVA server may restart. Whether it continues to pass network traffic during this time depends on the installation mode (Bridge, HTTP proxy, or ICAP).

System Maintenance

Go to **Administration > System Maintenance** to shut down or restart the system for maintenance purposes. IWSVA records the actions performed to the audit and system event logs.

Shut down—Select this option to turn off the appliance and stop the IWSVA service.

Restart—Select this option to restart the IWSVA service or the system. The IWSVA service is unavailable while the system is restarting.

Comment—Enter a reason for the selected action you want to perform. You cannot leave this field blank. The information you enter in this field is recorded in the logs.

Product License

The Product License function allows you to register and license IWSVA. Fully activating IWSVA is a two-step process. First, you must register IWSVA with Trend Micro. After registering, a valid IWSVA activation code (AC) will be provided to license the product.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support ("Maintenance") for one (1) year from the date of purchase only.

To activate IWSVA, you first need a Registration Key, which you acquire during product registration. It allows you to obtain an activation code. You can activate IWSVA using the Deployment Wizard or later using the IWSVA console.

License Expiration Warning

Typically, ninety (90) days before the Maintenance Agreement expires, you will start to receive email notifications, alerting you of the upcoming discontinuances. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

https://olr.trendmicro.com/registration/

Registering IWSVA

There are several ways to register IWSVA:

- *To register if you are a new customer:*
- *To register if you are a registered user:*

To register if you are a new customer:

1. Click the Trend Micro Product Registration Server link in your product at **Administration > Development Wizard > Product Activation**.
2. In the Enter Registration Key screen, use the Registration Key that came with your product (Trend Micro Enterprise Protection DVD or License Certificate).
3. Click **Continue**, and then **I CONFIRM**.

   The Confirm Product Information screen appears.
4. Click **Continue with Registration** to confirm all the product information.
5. Next, type all the required contact information in the fields provided and click **Submit**.
6. From the Confirm Registration Information screen, click **Edit** to update your contact information and click **OK** to continue.

   The Activation Code screen appears. Your Activation Code will be sent to your registered email address.
7. Click **OK** to finish.

To register if you are a registered user:

1. Click the Trend Micro Product Registration Server link in your product at **Administration > Development Wizard > Product Activation**.
2. Type your login ID and password in the fields provided, and then click **Login**.

   You will be prompted to change your password the first time you log on.
3. In the **My Products** screen, click **Add Products** and type the Registration Key.
4. To edit your company profile, click **View/Edit Company Profile**.
5. Your Activation Code appears on the next screen. To receive a copy of your Activation Code at your registered email address, click **Send Now**.

Note: For maintenance renewal, contact Trend Micro sales or your reseller. Click **Check Status Online** at **Administration > Product License** to manually update the maintenance expiration date on the Product License screen.

Obtaining a Registration Key

The Registration Key can be found on:

- Trend Micro Enterprise Solution DVD
- License Certificate (that you obtained after purchasing the product)

Registering and activating your copy of IWSVA entitles you the following benefits:

- Updates to the IWSVA pattern files and scan engine
- Technical support
- Easy access in viewing the license expiration update, registration and license information, and renewal reminders
- Easy access in renewing your license and updating the customers profile

Registration Keys have 18 characters and appear as follows:

```
xx-xxxx-xxxx-xxxx-xxxx
```

Obtaining and Entering an Activation Code

When the full version expires, IWSVA security updates will be disabled; when the evaluation period expires, both the security updates and scanning capabilities will be disabled. In the Product License screen, you can obtain an Activation Code online, view renewal instructions, and check the status of your product.

To activate IWSVA, you need an Activation Code. This can be done in several ways.

- You automatically receive an evaluation Activation Code if you download IWSVA from the Trend Micro Web site.
- You can use a Registration Key to obtain an Activation Code online.

Activation Codes have 31 characters and appear like this:

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

To obtain and enter an activation code online:

1. Open the IWSVA console and then click **Administration > Product License**.
2. Obtain an activation code by registering IWSVA (click the link at the top of the page to register and then follow the on-screen instructions).
3. Click the **Enter a new code** link.
4. When prompted, type the activation code in the Activation Code field and then click **Activate**.

Updating Your License

To obtain the latest license through the Web, go to **Administration > Product License** and click **Check Online Status**.

For more renewal instructions, see: https://olr.trendmicro.com/registration/us/en-us/instruction_renew.aspx

Renewing a Maintenance Agreement

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which you must purchase renewal maintenance.

If your Maintenance Agreement expires, scanning will still be possible, but virus pattern and program updates will stop. To prevent this, renew the Maintenance Agreement as soon as possible.

- To purchase renewal maintenance, contact the same vendor from whom you purchased the product. A Maintenance Agreement, extending your protection for a year, will be sent by post to the primary company contact listed in your company's Registration Profile.
- To view or modify your company's Registration Profile, log in to the account at the Trend Micro online registration Web site:

  https://olr.trendmicro.com/registration/us/en-us

Support

Using the case diagnostic tool (CDT), IWSVA generates core and/or system file(s) containing the system data held in memory when a process abnormally terminates. The Generate System Information File button is an extension of this feature, allowing you to package the current machine "state" at the click of a button.

The core and/or system file(s) that IWSVA generates contains the following information:

- **IWSVA information**—Includes the IWSVA product version, engine version, build number, and IWSVA hot fixes and service pack information. Product and integration settings are also part of this information

- **IWSVA/system logs**—Includes the IWSVA logs and debug logs, logs generated by syslogd daemon (if system logs are enabled), and core dump file
- **System/network information**—Includes the hardware configuration, operating system, build, system resource status, other applications installed, and network information
- **CDT-compliant configuration/plugins information**—Includes information about changes made to the CDT as a result of IWSVA adding a new component, such as a TMCM or MCP agent.

Core files are first created in the first directory listed as follows, and then compressed and moved to the second directory listed:

```
/var/iwss/coredumps
```

```
/var/iwss/UserDumps
```

Use these files when working with Trend Micro technical support to help diagnose the cause of your problem. To view the files yourself, use a program like GDB, the GNU Project debugger.

While IWSVA generates the core and/or system file(s), the application could encounter some conditions that prevent it from gathering all the possible diagnostic information. For instance, debug could be disabled, a core dump may not exist, or other critical commands or files may not exist. In this case, IWSVA gathers as much information as possible and also records any errors encountered in a log file with comprehensive messages.

Network Packet Capturing

The Network Packet Capturing wizard is located on the Administration > Support | Network Packet Capturing tab. Using the captured network packet, administrators or support teams can perform traffic debug or analysis.

With this feature, administrators can choose a single or multiple network interfaces on which to simultaneously capture network packet. After the capture starts, the elapsed time displays. The capture operation stops when the administrator clicks Stop capturing or when the (default) maximum file size of 10GB is reached.

Note: The default maximum file size limitation is configured in `/etc/iscan/network.ini`.

The packet capture for each interface will be save in an individual file using the naming convention of "capture-{interface}-{date:time}.pcap". For example capture-eth0-20111101:31:31:01.pcap would be the file name for the packet capture on the eth0 network interface performed on November 1, 2011.

After the network packet capture completes, all packet capture files are saved in one compressed package file named to "capture-{date}.tgz". This file displays in the downloadable list. Administrators can either download or deleted the compressed file.

Using Network Packet Capturing

Administrators can analyze traffic with this feature that allows packet captures for selected interfaces or a single interface.

To capture network packets:

1. Go to the **Administration > Support** page and click the **Network Packet Capturing** tab.
2. Select the appropriate interface(s) from the **Available** column.
3. Click **Add** or **Add All** to move the selected interfaces to the Selected column.
4. If needed, click **Remove** or **Remove All** to remove interfaces from the Selected column.
5. Click **Start Capturing**. The elapsed time displays. The capture stops when the maximum files size of 10GB is reached.
6. If necessary, click **Stop Capturing** to stop the packet capture before reaching the maximum file size.
7. When the capture finishes, select the appropriate generate file or select All.
8. Select an action:
   - Click **Download** and browse to save the capture file to a directory.
   - Click **Delete** to delete the generated files and click **OK**.

Chapter 14

Testing and Configuring IWSVA

After opening the InterScan Web Security Virtual Appliance (IWSVA) console, test the following to verify that the program is working properly. The following lists the tests described in this chapter:

EICAR Test File

The European Institute for Computer Antivirus Research (EICAR) has developed a test virus to test your antivirus appliance. This script is an inert text file. The binary pattern is included in the virus pattern file from most antivirus vendors. The test virus is not a virus and does not contain any program code.

WARNING! **Never use real viruses to test your Internet security.**

Download the EICAR test virus from the following URLs:

`http://www.eicar.org/anti_virus_test_file.htm`

`https://secure.eicar.org/eicar.com`

Alternatively, you can create your own EICAR test virus by typing or copying the following into a text file, and then naming the file `eicar.com`:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
$H+H*
```

Note: Flush the URL cache (**HTTP** > **Configuration** > **URL Cache**), the Content Cache (**HTTP > Configuration > Content Cache**), and your local browser before testing and local browser before testing. If either cache contains a copy of the test virus, it is possible an attempt to download the file would get the file from the cache, rather than getting it from the Internet, and IWSVA would not detect the file.

Testing Web Reputation

To test IWSVA's Web Reputation feature, open a Web browser and type the following in the address field:

```
http://wr21.winshipway.com
```

If the test is successful, you should receive an IWSVA Security Event message stating, "This URL has a Web security rating that prohibits it from being accessed."

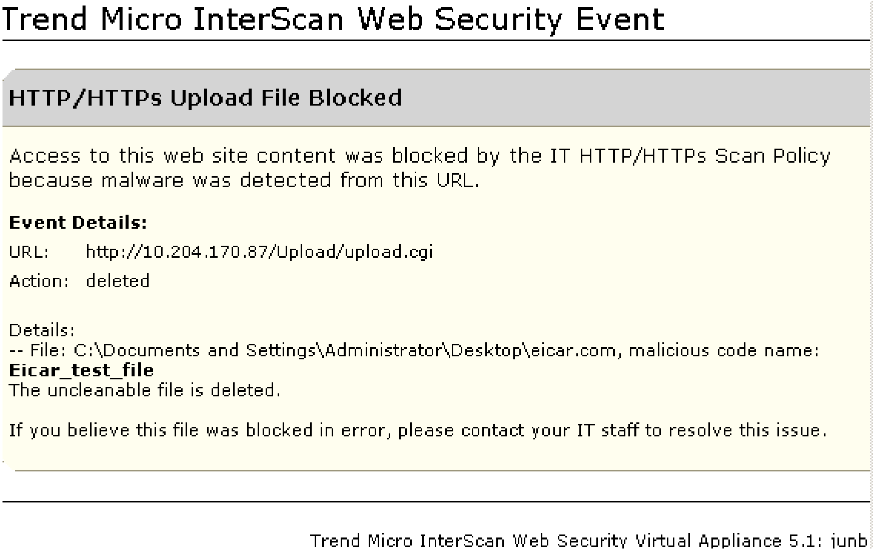
Testing Upload Scanning

The following procedure contains instructions to test the uploaded virus:

1. Open the IWSVA console and click **HTTP > HTTP Scan > Policies** in the main menu. Clear **Enable virus scanning**, and then click **Save**.
2. Download the test virus (eicar.com) from the following page:

   `http://www.eicar.org/anti_virus_test_file.htm`

3. Save the test virus on your local machine.
4. Re-open the IWSVA console, under **HTTP > HTTP Scan > Policies** in the main menu, select **Enable virus scanning**, and then click **Save**.
5. Upload the test virus to a Web site. A message similar to *Figure 14-1* appears in your browser.



Trend Micro InterScan Web Security Event

HTTP/HTTPs Upload File Blocked

Access to this web site content was blocked by the IT HTTP/HTTPs Scan Policy because malware was detected from this URL.

Event Details:

URL: http://10.204.170.87/Upload/upload.cgi

Action: deleted

Details:
-- File: C:\Documents and Settings\Administrator\Desktop\eicar.com, malicious code name: **Eicar_test_file**
The uncleanable file is deleted.

If you believe this file was blocked in error, please contact your IT staff to resolve this issue.

Trend Micro InterScan Web Security Virtual Appliance 5.1: junb

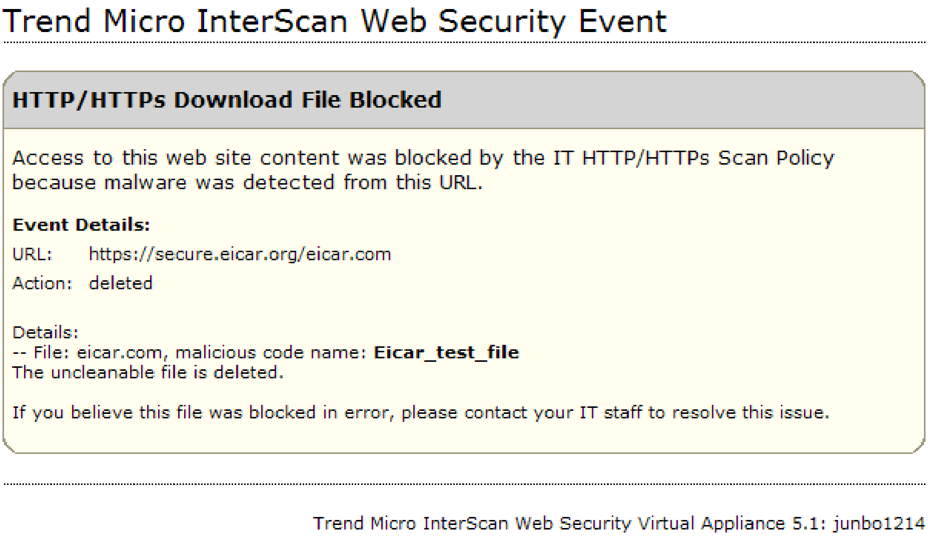
FIGURE 14-1. This warning screen shows the detection of an EICAR test virus.

Testing HTTPS Decryption Scanning

This section describes the procedure to test HTTPS decryption on IWSVA in stand-alone mode.

To test virus scanning of decrypted HTTPS traffic:

1. Set the Web client's HTTP proxy to point to IWSVA (for example, open Internet Explorer and click **Tools > Internet Options > Connections > LAN Settings > Use a proxy server**).
2. Open the IWSVA Web console and click **HTTP > HTTPS Decryption > Settings | Server Certificate Validation** and make sure all options are selected.
3. Click **HTTP > HTTPS Decryption > Policies** and click **Enable HTTPS Decryption**.
4. Click **Add** to create a new HTTPS decryption policy. In the Rules tab, select **Disease Vector** under the Business: Computer/Internet category.
5. From the client machine, access the test virus file from the following URL:
   ```
   https://secure.eicar.org/eicar.com
   ```
6. Because the server certificate is not in the trusted list on IWSVA, a certificate error notification displays. Click **Visit site anyway**.
7. A security warning screen displays. The warning message varies depending on whether URL filtering is also enabled or not.



Trend Micro InterScan Web Security Event

HTTP/HTTPs Download File Blocked

Access to this web site content was blocked by the IT HTTP/HTTPs Scan Policy because malware was detected from this URL.

Event Details:

URL: https://secure.eicar.org/eicar.com

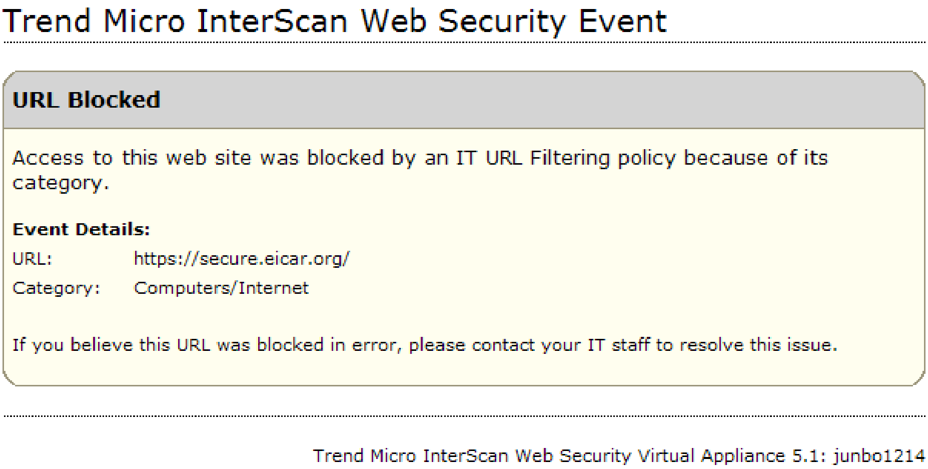
Action: deleted

Details:
-- File: eicar.com, malicious code name: **Eicar_test_file**
The uncleanable file is deleted.

If you believe this file was blocked in error, please contact your IT staff to resolve this issue.

Trend Micro InterScan Web Security Virtual Appliance 5.1: junbo1214

FIGURE 14-2. Security warning screen if URL filtering is disabled



Trend Micro InterScan Web Security Event

URL Blocked

Access to this web site was blocked by an IT URL Filtering policy because of its category.

Event Details:

URL: https://secure.eicar.org/

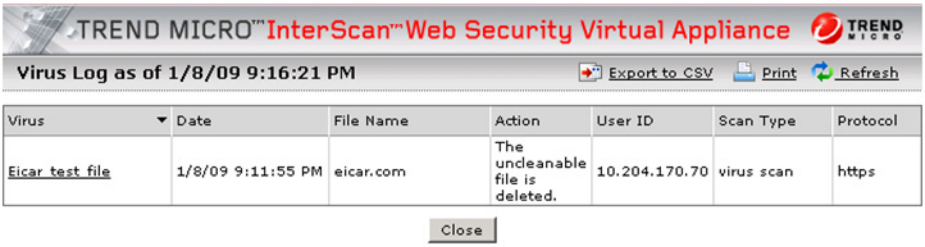
Category: Computers/Internet

If you believe this URL was blocked in error, please contact your IT staff to resolve this issue.

Trend Micro InterScan Web Security Virtual Appliance 5.1: junbo1214

FIGURE 14-3. Security warning screen if URL filtering is also enabled

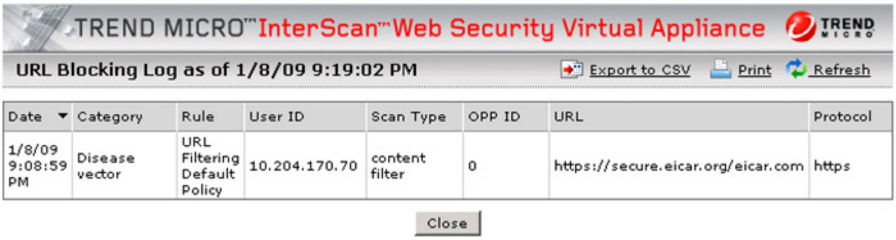
On the IWSVA server, you can view detailed log information in the URL filtering log or the virus log.



Virus Log as of 1/8/09 9:16:21 PM

Virus	Date	File Name	Action	User ID	Scan Type	Protocol
Eicar test file	1/8/09 9:11:55 PM	eicar.com	The uncleanable file is deleted.	10.204.170.70	virus scan	https

FIGURE 14-4. View the log for HTTPS decryption test in the Virus Log screen if URL filtering is disabled



URL Blocking Log as of 1/8/09 9:19:02 PM

Date	Category	Rule	User ID	Scan Type	OPP ID	URL	Protocol
1/8/09 9:08:59 PM	Disease vector	URL Filtering Default Policy	10.204.170.70	content filter	0	https://secure.eicar.org/eicar.com	https

FIGURE 14-5. View the log for HTTPS decryption test in the URL Filtering Log screen if URL filtering is enabled

Testing FTP Scanning

The following procedure contains instructions to test your FTP virus scanning capability in standalone mode.

To test virus scanning of FTP traffic:

1. Download the test virus from the following page:

   `http://www.eicar.org/anti_virus_test_file.htm`

2. Access the FTP server through IWSVA with it working as the FTP proxy.

For example, assume the following IP addresses: IWSVA FTP proxy server (`10.2.203.126`), FTP server (`10.2.202.168`).

Open a command line prompt and type the following:

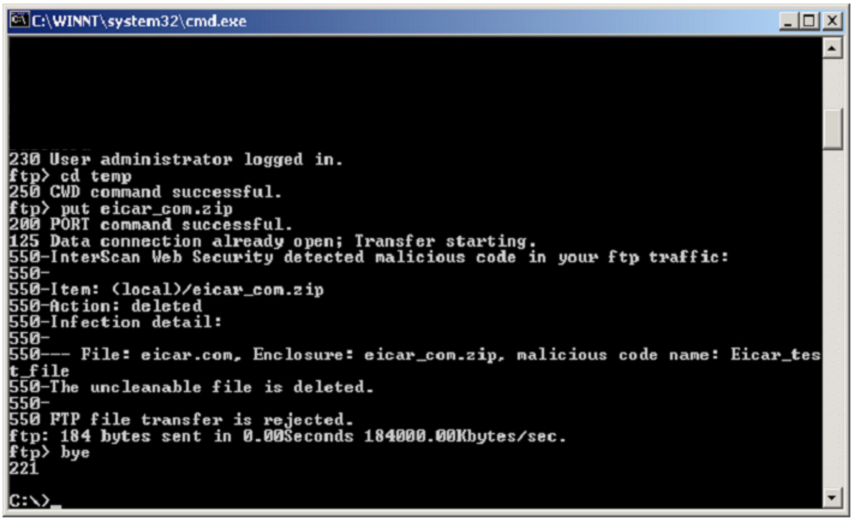
```
ftp 10.2.203.126
```

3. Log on as `user@host`. For example, if your FTP account name is `anonymous` and the IP address of the FTP server is `10.2.202.168`, then log on as `anonymous@10.2.202.168`

4. Upload the test virus (for example, eicar_com.zip) by typing the following command:

   ```
   put eicar_com.zip
   ```

5. If you have configured the IWSVA FTP proxy mode correctly, IWSVA displays a message similar to the one in *Figure 14-6*.



```
230 User administrator logged in.
ftp> cd temp
250 CWD command successful.
ftp> put eicar_com.zip
200 PORT command successful.
125 Data connection already open; Transfer starting.
550-InterScan Web Security detected malicious code in your ftp traffic:
550-
550-Item: (local)/eicar_com.zip
550-Action: deleted
550-Infection detail:
550-
550--- File: eicar.com, Enclosure: eicar_com.zip, malicious code name: Eicar_tes
t_file
550-The uncleanable file is deleted.
550-
550 FTP file transfer is rejected.
ftp: 184 bytes sent in 0.00Seconds 184000.00Kbytes/sec.
ftp> bye
221

C:\>_
```

FIGURE 14-6. This is a warning message that shows the detection of a virus in eicar_com.zip.

Testing URL Monitoring

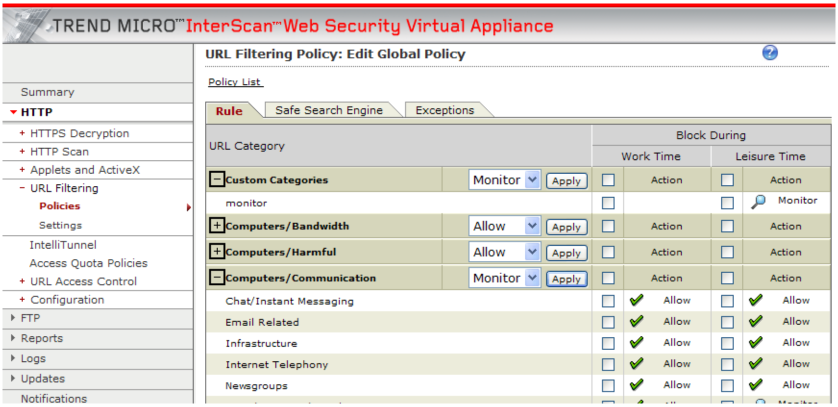
Before testing the monitor feature in URL filtering, require your users to set the Web client's HTTP proxy to point to IWSVA.

To test URL filtering:

1. Open the IWSVA Web console and click **HTTP > Configuration > Custom Categories** and create a new category **"monitor"** for the following URL:

   ```
   http://www.download.com
   ```

2. Click **HTTP > URL Filtering > Policies** and select **Enable URL Filtering**; then, click **URL Filtering Global Policy** to edit the policy.
3. In the Rule tab, select **Monitor** and click the check box under Leisure Time for "monitor" under Custom Categories; then, click **Apply**.
4. Select **Monitor** and click the check box under Leisure Time for Search Engines/Portals under Computers/Communications; then, click **Apply**.



URL Filtering Policy: Edit Global Policy

Policy List

URL Category			Block During			
			Work Time		Leisure Time	
Custom Categories	Monitor	Apply	□	Action	□	Action
monitor			□		□	Monitor
Computers/Bandwidth	Allow	Apply	□	Action	□	Action
Computers/Harmful	Allow	Apply	□	Action	□	Action
Computers/Communication	Monitor	Apply	□	Action	□	Action
Chat/Instant Messaging			□	✓ Allow	□	✓ Allow
Email Related			□	✓ Allow	□	✓ Allow
Infrastructure			□	✓ Allow	□	✓ Allow
Internet Telephony			□	✓ Allow	□	✓ Allow
Newsgroups			□	✓ Allow	□	✓ Allow

FIGURE 14-7. Rule screen configuration for URL monitor testing

5. Save and deploy this policy.

6. From a client computer, access the following Web sites during leisure time:

    `http://www.download.com`

    `http://www.google.com`

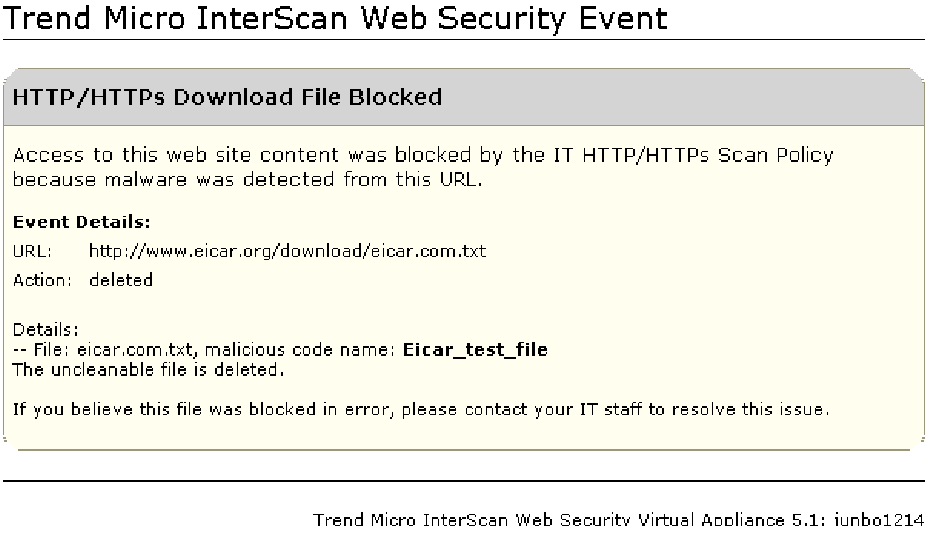
    `http://www.yahoo.com`

You should be able to access the Web sites without seeing any warning messages. To query and view URL filtering log, access the IWSVA Web console and click **Logs > Log Query > URL Filtering Log**.

Testing Download Scanning

To test virus scanning when downloading using HTTP or FTP over HTTP, attempt to download the test virus from the following Web site:

`http://www.eicar.org/anti_virus_test_file.htm`



Trend Micro InterScan Web Security Event

HTTP/HTTPs Download File Blocked

Access to this web site content was blocked by the IT HTTP/HTTPs Scan Policy because malware was detected from this URL.

Event Details:

URL: http://www.eicar.org/download/eicar.com.txt

Action: deleted

Details:
-- File: eicar.com.txt, malicious code name: **Eicar_test_file**
The uncleanable file is deleted.

If you believe this file was blocked in error, please contact your IT staff to resolve this issue.

Trend Micro InterScan Web Security Virtual Appliance 5.1: iunbo1214

FIGURE 14-8. This virus-warning screen opens if the system is set up properly.

If a client attempts to download an infected file, IWSVA blocks all other users' access to that site for four hours by default. When other clients subsequently attempt to access the same URL that contained the virus, they will see a URL blocking message instead of the virus-warning message.

Configure the default block time (in hours) by changing the parameter `infected_url_block_length` under the `[Scan-configuration]` section of the `intscan.ini` file.

Testing URL Filtering

Trend Micro recommends that you use the default settings to test URL filtering.

To test URL Filtering:

1. Click **HTTP > URL Filtering > Settings** from the main menu and in the **Schedule** tab. Configure the work days and times.
2. Click **HTTP > URL Filtering > Policies** from the Main menu.
3. Select **Enable URL filtering** and then click **Save**.
4. Click **URL Filtering Global Policy** and select the Block action to apply to the categories that you want blocked during work and leisure times.

   Keep the default settings in the Safe Search and Exception tabs.
5. Click **Save** to save any changes. Click **Deploy Policies** to make the policy effective immediately.
6. Open a browser and access any site that is in a category to be blocked at the time of the test. IWSVA blocks access to URLs belonging to the category that is set to be blocked.

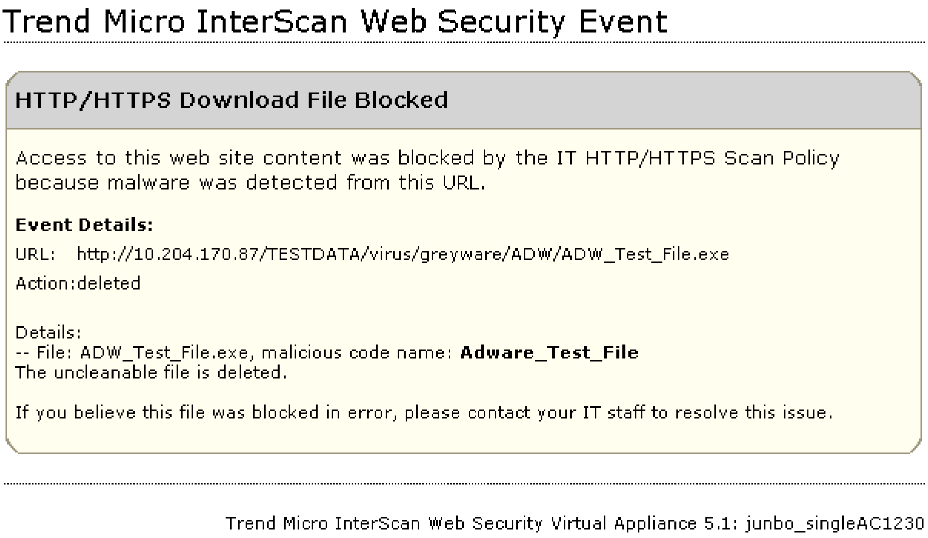
Testing Spyware Scanning

To test spyware scanning:

1. Click **Summary** from the main menu.
2. Click the **Scanning** tab.
3. Enable spyware and other grayware categories for scanning by clicking **HTTP scanning**.

4. Click **HTTP > HTTP Scan > Policies**.
5. Click **Virus Scan Global Policy**.
6. Click the **Spyware/Grayware Scan Rule** tab and then select the types of spyware/grayware that should be scanned.
7. Click **Save**.
8. Click **Virus Scan Global Policy**.
9. Click the **Action** tab.
10. Under the **Uncleanable files** field, select the action setting (Delete, Quarantine, or Pass).
11. Click **Save**.
12. Click **Deploy Policies** to make the policy effective immediately.

    After a successful spyware detection, a sample message appears:



Trend Micro InterScan Web Security Event

HTTP/HTTPS Download File Blocked

Access to this web site content was blocked by the IT HTTP/HTTPS Scan Policy because malware was detected from this URL.

Event Details:

URL: http://10.204.170.87/TESTDATA/virus/greyware/ADW/ADW_Test_File.exe

Action:deleted

Details:
-- File: ADW_Test_File.exe, malicious code name: **Adware_Test_File**
The uncleanable file is deleted.

If you believe this file was blocked in error, please contact your IT staff to resolve this issue.

Trend Micro InterScan Web Security Virtual Appliance 5.1: junbo_singleAC1230

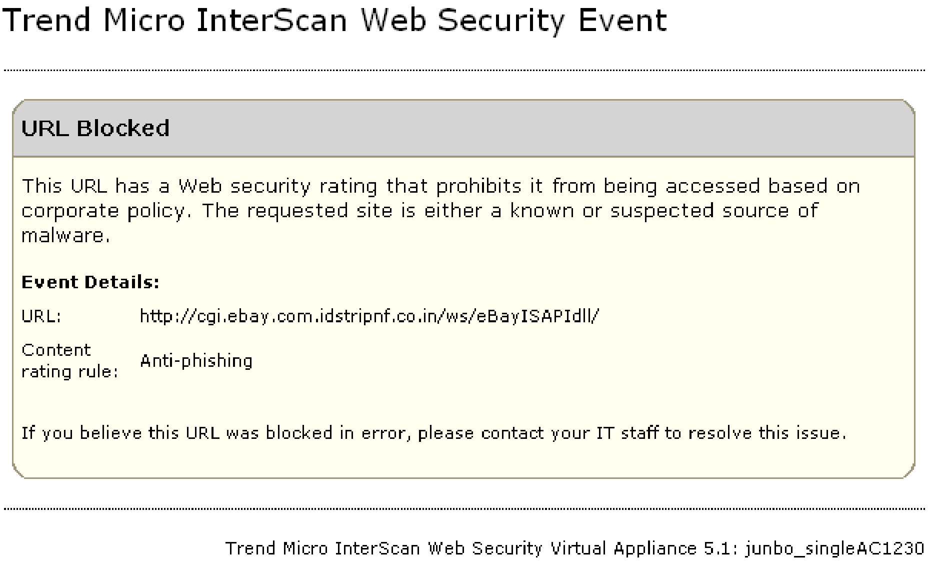
FIGURE 14-9. A sample message after detecting a spyware with action "Delete" setting

Testing PhishTrap

Procedure:

1. Click **HTTP > URL Access Control > URL Blocking** from the main menu.
2. Select **Enable URL blocking**.
3. Click the **Via Pattern File Phish** tab.
4. Under **Block the following Phish categories**, select all four categories (Phishing, Spyware, Virus accomplice, and Disease vector).
5. Click **Save**.

   After a successful phishing site detection, a sample message appears:



Trend Micro InterScan Web Security Event

URL Blocked

This URL has a Web security rating that prohibits it from being accessed based on corporate policy. The requested site is either a known or suspected source of malware.

Event Details:

URL: http://cgi.ebay.com.idstripnf.co.in/ws/eBayISAPIdll/

Content rating rule: Anti-phishing

If you believe this URL was blocked in error, please contact your IT staff to resolve this issue.

Trend Micro InterScan Web Security Virtual Appliance 5.1: junbo_singleAC1230

FIGURE 14-10. A sample message after detecting a phishing site.

Testing Java Applet and ActiveX Scanning

Java applets and ActiveX controls are used on many Web pages to display interactive content or applications. One way to test IWSVA is to temporarily configure the global policy to block all applets and ActiveX controls, and then attempt to open Web pages that use them (to verify that the applet or object is blocked).

To test Java applet and ActiveX scanning:

1. Click **HTTP > Applets and ActiveX > Policies** from the main menu.
2. If necessary, select **Enable Applet/ActiveX security** and click **Save**.
3. Click **Applet/ActiveX Security Global Policy**.
4. On the **Java Applet Security Rules** tab, click **Block all Java applets** and then **Save**.
5. On the **ActiveX Security Rules** tab, click **Block all cabinet files** and **Block all PE format files** and then click **Save**.
6. From the **Applets and ActiveX Policies** screen, select **Deploy Policies Now** to make policy changes effective immediately.
7. Open a Web browser and attempt to navigate to Web sites that use Java applets and ActiveX controls, for example, for stock price tickers or games.

   IWSVA blocks the mobile code from downloading and running in your browser.

Note: Blocking all Java applets and ActiveX controls might be too restrictive for your environment because it prevents many legitimate Web sites from functioning properly. After testing, Trend Micro recommends going back to the **Applets and ActiveX Policy: Edit Global Policy** screen to change the settings back to the default or your own less-restrictive configuration.

Additional IWSVA Configurations

This section briefly introduces some common IWSVA configuration tasks.

Configuring the Separate Management Interface

In many large enterprises and/or secure networking environments, a separate network segment (also known as the management network) can be used to manage various network devices. For security reasons, the management network is not connected to the Internet and is a separate network that ordinary users are not allowed to access.

On the IWSVA server, you can enable the separate management interface that connects to the company's management network. A separate network interface must be available on the IWSVA server for the dedicate management interface. After the management interface is activated and configured on IWSVA, you can access the IWSVA Web console or CLI through the separate management interface. The following shows an example network topology:

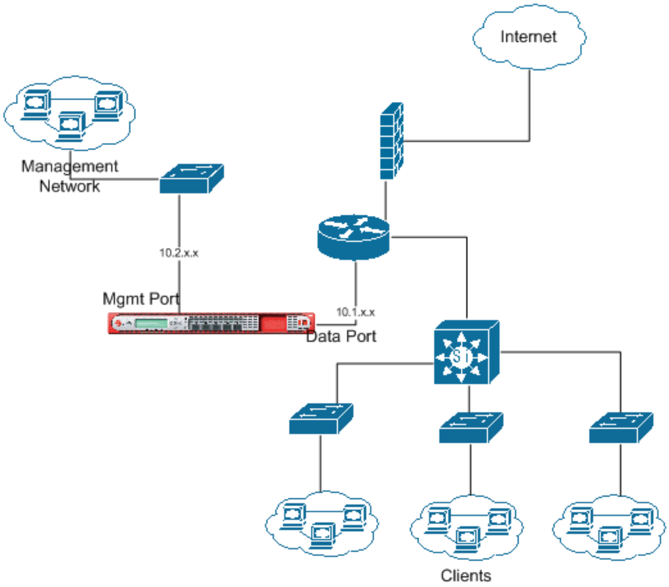


FIGURE 14-11. IWSVA management interface placement in the network

In this example, the management interface on the IWSVA is connected to the management network in the company. The clients access the Internet through the data (bridge or proxy) interface.

WARNING! **Do NOT configure the data (bridge/proxy) interface and the management interface to be in the same network segment. If they are in the same network segment, the firewall might block the HTTP(s) and FTP traffic.**

To configure the separate management interface:

1. From the main menu, click the **Administration > Deployment Wizard > Network Settings** page and then click the **Enable Separate Management Interface** check box.
2. From the **Ethernet interface** drop-down list, select a desired interface for the management interface.
3. Configure the IP address settings.
4. Select **Enable PING** if you want IWSVA to respond to PING requests on this interface.
5. Click **Save**. You can access the separate management interface to log into the Web console and manage IWSVA.

Tip: If the IWSVA machine is behind a router/switch in the management network, configure a static route on the management interface to access IWSVA through the Web console or SSH.

To test the separate management interface:

1. First try to log on to the Web console through the data (bridge or proxy) interface. You should be able to log on and manage IWSVA.
2. Next try accessing the Web console on the separate management interface. You should be able to log on and manage IWSVA.

Securing the IWSVA Console

By default, the IWSVA Web management console (GUI) is accessed through an HTTP connection on port 1812. For improved security, Trend Micro recommends that you use a Secure Socket Layer connection (HTTPS). You will need to provide a public key and certificate.

To connect to the IWSVA Web console through HTTPS:

1. From the main menu, click **Administration > Network Configuration > Web Console** and choose **SSL Mode** to enable a secure connection to the IWSVA console.
2. In the **SSL Certificate** field, click **Browse** to locate the certificate you will use, and then **Upload** to import it to the IWSVA device.
3. Type the password associated with the SSL certificate, if any.
4. Type the port on which you would like to open the IWSVA console and then click **Save**.

   For example:

   ```
   https://<IWSVA device IP address:port>
   ```

Note: **Non-SSL mode** is the default; use it to access the IWSVA console using a non-secure URL; for example:

```
http://<IWSVA device IP address:port>
```

The default non-secure port is 1812; you can change it to any unused port (recognized by the firewall).

Activating Remote CLI

You can enable the remote CLI feature to connect to the IWSVA server and configure settings using the CLI commands. Remote connection is secured through SSH v2 (Secure SHell) which is a network protocol that allows two network devices to exchange data in a secured connection. SSH replaces Telnet which sends data (including passwords) in clear text.

To enable remote CLI on the IWSVA server:

1. From the main menu, click **Administration > Network Configuration > Remote CLI** and choose **SSH: Command line access** to enable remote CLI access using SSH on IWSVA.
2. Type the service port number for SSH v2. The default port number is 22.
3. Click **Save**.

Specifying HTTP Scanning

HTTP scanning is enabled by default. The HTTP traffic flow for clients to browse the Web and perform other HTTP operations can be enabled and disabled (see Enabling the HTTP(s) Traffic Flow on page 5-2).

Specifying the User Identification Method

IWSVA supports several methods to identify clients when configuring a policy's scope (see Configuring the User Identification Method on page 6-5). The default identification method is through the client's IP address. IWSVA also supports identifying clients through their host names or MAC addresses and through their LDAP directories.

Enabling the Guest Account (LDAP only)

When using the **User/group name authentication** identification method, all virus scanning, Java applets and ActiveX security, URL filtering, and access quota policies will support configuring policies for users who are temporarily visiting your network. These guest policies are applied to clients that connect to IWSVA through the "guest" port. The guest account is disabled by default—enable it to allow guests Internet access.

To enable the guest account and configure the guest port:

1. IWSVA needs to be configured for User/group name authentication (LDAP) in the **HTTP > Configuration > User Identification | User Identification** tab.
2. To enable the guest account, go to **Administration > Deployment Wizard > Start > Deployment Mode**.
3. Select **Forward proxy mode** and click **Next**.
4. On the Proxy Settings screen, in the Forward Proxy Mode section, select the **Enable guest account** check box.

The default value in the **Port number** field is 8081 and typically does not have to be modified unless the port is already in use.

5. Click **Next** until the Submit button displays. Click **Submit** and then click **Close**.

Reviewing Scanning and Filtering Policies

IWSVA is pre-configured to provide a baseline level of gateway security. Trend Micro recommends reviewing the HTTP virus scanning Global and Guest policy configurations to ensure they reflect your organization's security policies.

Additionally, if you are running the Applets and ActiveX security, URL filtering and FTP scanning modules, review those configurations and modify them accordingly.

Enabling Access Quota Policies

To limit bandwidth consumption, enable the access quota control to set a maximum amount of data that a client can retrieve or download during a given time period.

To enable access quota control:

1. Click **HTTP > Access Quota Policies** on the main menu.
2. Select **Enable access quota control**.
3. To configure access quota control for your network's guest users, click **Access Quota Guest Policy** and configure the settings. To configure access quota control for other network users, click **Add** and configure a new policy.
4. Click **Save**.

   For the new policy to take effect immediately, click **Deploy Policies** in the **HTTP > Access Quota Policies** page.

Setting Access Control Settings

The default IWSVA settings allow all non-guest clients to access the Internet. To allow a subset of your clients Internet access, configure the IP addresses allowed to do so on the **Internet Access Control** screen.

In addition, IWSVA can be configured to exempt some servers from scanning, URL filtering, and URL blocking to speed up browsing performance when visiting trusted sites. For example, consider adding the IP address ranges of your intranet sites to the Server IP white list to exempt frequently visited sites from scanning and filtering.

To configure which clients are allowed to access the Internet:

1. Click **HTTP > Configuration > Internet Access Control** from the main menu.
2. On the **Client IP** tab, select **Enable HTTP access based on client IP** and enter the IP addresses that are allowed to access the Internet.
3. Click **Save**.

To configure which servers are exempt from filtering and scanning:

1. Click **HTTP > Configuration > Internet Access Control** from the main menu.
2. Click the **Server IP White List** tab, configure the IP addresses of servers that are exempt from scanning, URL filtering, and URL blocking.
3. Click **Save**.

Adding System Updates or Removing an Application Patch

From time to time, Trend Micro makes updates available through the Download Center. After downloading the latest update from the Download Center to a desktop or other computer, you can upload it to the IWSVA device where it is automatically installed.

To add a system update:

1. Download the latest update from http://downloadcenter.trendmicro.com
2. From the main menu, click **Administration > System Updates** and then click **Browse**.
3. Locate the update you downloaded from the Trend Micro Download Center.
4. Click **Upload** to have IWSVA copy the update to the IWSVA device and begin installing.

   Only a properly formatted and encrypted Trend Micro patch can be uploaded from this utility.

To remove an application patch:

1. From the main menu, click **Administration > System Updates**.
2. In the History section, click the **Application Patches** tab.
3. Click the **Uninstall** link beside the application patch number.
4. In the preview page that appears, verify the version of the patch you want to remove.

   You can remove the most recently installed application patch at any time.
5. Click **Uninstall**. A progress page appears. After the patch has been removed, close the window to return to the main IWSVA console.

About Hot Fixes, Patches, and Service Packs

After an official product release, Trend Micro often develops hot fixes, patches, and service packs to address issues, enhance product performance, or add new features.

The following is a summary of the items Trend Micro might release:

- **Hot fix**: A work around or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore, not released to all customers. Windows hot fixes include a setup program.
- **Security Patch**: A hot fix focusing on security issues that is suitable for deployment to all customers.
- **Patch**: A group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis.
- **Service Pack**: A consolidation of hot fixes, patches, and feature enhancements significant enough to be considered a product upgrade. You can obtain hot fixes from your Technical Account Manager. Check the Trend Micro Knowledge Base to search for released hot fixes:

  - http://esupport.trendmicro.com/support/

  Check the Trend Micro Web site regularly to download patches and service packs:

  - http://www.trendmicro.com/download

  All releases include a readme file with the information you need to install, deploy, and configure your product. Read the readme file carefully before installing the hot fix, patch, or service pack file(s).

Checking the Database Connection

When you are setting up a database for multiple IWSVA configurations, specify the same database for all IWSVA devices.

To check the database connection settings:

1. Click **Administration > IWSVA Configuration > Database Connection**.
2. Under **Database Connection Settings**, view the database settings.
3. Click **Test Database Connection**.

Policy settings are stored in the database, and IWSVA copies the settings to a memory cache. IWSVA reloads the settings from the database into memory according to the Policy Deployment Settings (in minutes) option that specifies the interval.

To configure the Policy Deployment Settings (in minutes):

1. Open the IWSVA Web console and click **Administration > IWSVA Configuration > Policy Deployment**.
2. Under **Policy Deployment Settings (in minutes)**, type a value for the following parameters:
   - Access quota policy
   - HTTPS policy
   - Applets and ActiveX policy
   - IntelliTunnel policy
   - URL filtering policy
   - Virus scan policy
3. Click **Save**.

Changing the Management Console Password

The Web console password is the primary means to protect your IWSVA device from unauthorized changes. For a more secure environment, change the console password on a regular basis and use a password that is difficult to guess.

The administrator passwords can be changed through the Web console interface. The CLI allows you to change the Enable, Root, and any Administrator account passwords. The CLI command uses the “configure password” command to make the changes.

To change the Web console password through the CLI:

1. Log in to the CLI console as "enable."
2. Type the following command:
   ```
   configure system password
   ```

The following tips help you design a safe password:

- Include both letters and numbers in your password
- Avoid words found in any dictionary, of any language
- Intentionally misspell words
- Use phrases or combine words
- Use both uppercase and lowercase letters

To change the Web console password:

1. Open the IWSVA console and click **Administration > Management Console > Account Administration** in the main menu.
2. Click the user account for which you want to change the password.
3. From the Login Accounts page, type the new password in the **Password** field and then again in the **Confirm Password** field.
4. Click **Save**.

Configurations After Changing the Web Console Listening Port

When users enable the HTTPS Web console management mode by accessing the **Administration > Network Configuration > Web Console** screen and setting the **Port number** for SSL mode to a port (such as 8443) not used by other applications, they should also specify this SSL management port number in the **HTTP > Configuration > Internet Access Control** screen as well (see Using SSL with Damage Cleanup Services (DCS) on page 14-23).

If this port number is not specified in the **Internet Access Control** screen, the consequence could be that the IWSVA progress page is blocked by IWSVA itself, when using the HTTPS Web console. In other words, when clients try to access URLs, they would see the progress bar blocked by IWSVA.

Using SSL with Damage Cleanup Services (DCS)

To redirect clients to DCS to clean up malicious code when you are using the HTTPS-enabled Web console, access to the secure port that IWSVA uses (typically 8443) must be enabled. Otherwise, redirection to DCS is not successful, because the redirection request is blocked.

To allow access to secure port 8443:

1. Click **HTTP > Configuration > Internet Access Control**, and make the **HTTPS Ports** tab active.
2. **Allow** access to the **Port** used for HTTPS traffic (typically 8443).
3. Click **Add** and then **Save**.

In addition, two parameters in the `[http]` section of the `intscan.ini` file need to be modified when IWSVA is configured to use HTTPS:

```
iscan_web_server=[user defined https port, e.g., 8443]

iscan_web_protocol=https
```

Verifying URL Filtering Settings

If you are running the URL filtering module, review the post-install tasks that follow to prepare IWSVA for your environment.

IWSVA accesses the Web Reputation database that contains URLs in over 80 categories, such as “gambling,” “games,” and “personals/dating.” These categories are contained in logical groups.

Trend Micro recommends reviewing the URL filtering settings to ensure that the categories that qualify as company-prohibited sites reflect the values of your organization and do not affect your employees’ business-related Web browsing. Before rolling out URL filtering policies, Trend Micro recommends verifying that the default categorizations are appropriate for your organization. For example, a clothing retailer might need to remove a swimsuit Web site from the “Intimate Apparel/Swimsuit” category located in the *Adult* group in order to allow legitimate market and competitor research.

Additionally, you might need to configure URL exceptions to enable employee access to specific sites that would otherwise be blocked, and review the definitions of “work time” to ensure it reflects your workplace schedule.

To review URL filtering settings:

1. Click **HTTP > URL Filtering > Policies > policy > Exceptions** from the main menu.
2. Choose an approved URL list from the drop-down list that contains the Web sites that will be exempt from URL filtering so that they are always accessible to your clients.
3. On the **Schedule** tab, the default setting for "work time" is Monday to Friday, from 08:00 to 11:59, and from 13:00 to 17:00. Modify these time settings according to the employee schedules in your workplace.
4. Click **HTTP > URL Filtering > Policies** from the main menu and review the category settings of the URL Filtering Guest Policy and URL Filtering Global Policy.

IWSVA Performance Tuning

If you are experiencing issues with slow browsing performance, consider the modifications described in the following section.

LDAP Performance Tuning

When running IWSVA to use the user/group name authentication identification method (LDAP), HTTP proxy performance becomes dependent upon the responsiveness of the LDAP directory server. In a worst case scenario, every HTTP request would require an LDAP query to authenticate the user's credentials, and another to retrieve group membership information for that user. These queries introduce latency in terms of the transmit/receive delay between IWSVA and the LDAP server, and add load to the LDAP server itself.

LDAP Internal Caches

To reduce the amount of LDAP queries required, IWSVA provides several internal caches:

- **User group membership cache:** This cache can store the group membership information for several hundred users. By default, entries in this cache are valid for 48 hours, or until the cache fills (at which point entries are replaced, starting with the oldest). The time to live (TTL) for entries in this cache can be configured through the ***`user_groups_central_cache_interval`*** setting in the ***`[user-identification]`*** section of the ***`intscan.ini`*** configuration file.
- **Client IP to User ID cache:** This cache associates a client IP address with a user who recently authenticated from that same IP address. Any request originating from the same IP address as a previously authenticated request is attributed to that user, provided the new request is issued within a configurable window of time (15 minutes by default for HTTP, 90 minutes for ICAP) from that authentication. The caveat is that client IP addresses recognized by IWSVA must be unique to a user within that time period; therefore, this cache is not useful in environments where there is a proxy server or source NAT between the clients and IWSVA, or where DHCP frequently reassigns client IPs. To enable or disable this cache, change the ***`enable_ip_user_cache`*** setting in the ***`[user-identification]`*** section of the ***`intscan.ini`*** configuration file. To change the TTL of this cache, change the ***`ip_user_central_cache_interval`*** (unit is hours). For example, to create a TTL of 30 minutes, enter “0.5”.
- **User authentication cache:** This avoids re-authenticating multiple HTTP requests passed over a persistent connection. When users pass the credential validation over a persistent connection, IWSVA adds an entry (two important keys in one cache entry are the client’s IP address and the client’s user name) in the user authentication cache so the subsequent requests over a keep-alive connection does not authenticate again. The client’s IP address and client’s user name serve as two forward references, or links, to the “client IP to user ID cache” and “user group membership cache,” respectively. IWSVA is still able to retrieve the user’s connection information from both the IP-user and user-group caches.

When deploying IWSVA with LDAP integration, it is important to consider the additional load that authenticating HTTP requests places on the LDAP directory server. In an environment that cannot effectively use the client IP to user ID cache, the directory server needs to be able to handle queries at the same rate IWSVA receives HTTP requests.

Disable Verbose Logging When LDAP Enabled

Trend Micro recommends turning off verbose logging in the `intscan.ini` file, under the ***[http]*** section, "verbose" parameter, when LDAP is enabled for server performance reasons. Verbose logging is primarily used by software developers to identify abnormal application behavior and troubleshooting. In a production deployment, verbose logging is usually unnecessary.

If verbose logging is enabled and LDAP is also enabled, IWSVA logs user authentication information and group membership information in the HTTP log in the Log folder. Logs might contain hundreds of lines per user and, therefore, significantly consume disk space, depending on the amount of internal traffic and the number of groups with which a user is associated. Verbose logging keeps the service busy by issuing I/O operations to the operating system. This might prevent the service from responding to HTTP requests in a timely fashion, and latency might occur. In an extreme bursting HTTP traffic environment, it's possible to observe significant delays when IWSVA starts up in the verbose mode.

Appendix A

Contact Information and Web-based Resources

This appendix provides information to optimize the InterScan Web Security Virtual Appliance (IWSVA) performance and get further assistance with any technical support questions you might have.

Topics in this appendix include:

Contacting Technical Support

In the United States, Trend Micro representatives can be reached through phone, fax, or email. Our Web site and email addresses is as follows:

http://www.trendmicro.com
http://esupport.trendmicro.com/
support@trendmicro.com

General US phone and fax numbers are as follows:

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Our US headquarters are located in the heart of Silicon Valley:

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014

To obtain Trend Micro contact information for your region/country, please visit http://www.trendmicro.com

IWSVA Core Files for Support

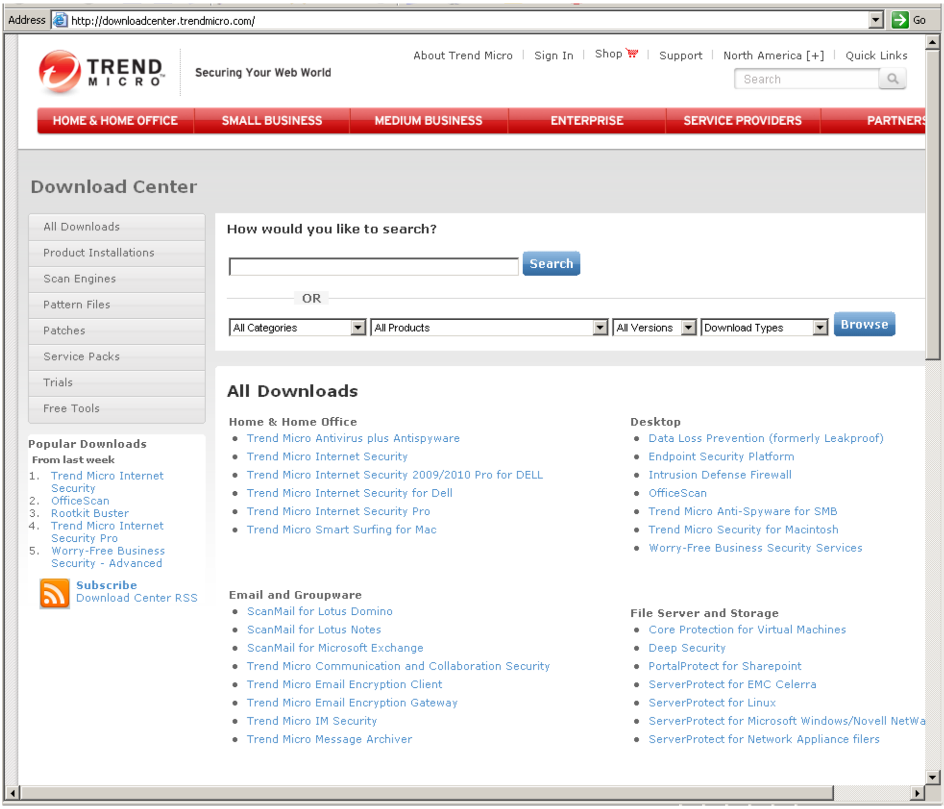
IWSVA generates a core file containing the system data held in memory when a process is abnormally terminated.

Raw core files are created in the `var/iwss/coredumps` directory on the IWSVA device. They are then compressed and moved to `/var/iwss/UserDumps`. You can use these files when working with Trend Micro technical support to help diagnose the cause of the problem.

To access the core files:

- From the main IWSVA menu, click **Administration > Support**.

To inspect the files yourself, use a program like GDB, the GNU Project debugger.



Download Center

How would you like to search?

Popular Downloads
From last week

1. Trend Micro Internet Security
2. OfficeScan
3. Rootkit Buster
4. Trend Micro Internet Security Pro
5. Worry-Free Business Security - Advanced

All Downloads

Home & Home Office

- Trend Micro Antivirus plus Antispyware
- Trend Micro Internet Security
- Trend Micro Internet Security 2009/2010 Pro for DELL
- Trend Micro Internet Security for Dell
- Trend Micro Internet Security Pro
- Trend Micro Smart Surfing for Mac

Email and Groupware

- ScanMail for Lotus Domino
- ScanMail for Lotus Notes
- ScanMail for Microsoft Exchange
- Trend Micro Communication and Collaboration Security
- Trend Micro Email Encryption Client
- Trend Micro Email Encryption Gateway
- Trend Micro IM Security
- Trend Micro Message Archiver

Desktop

- Data Loss Prevention (formerly Leakproof)
- Endpoint Security Platform
- Intrusion Defense Firewall
- OfficeScan
- Trend Micro Anti-Spyware for SMB
- Trend Micro Security for Macintosh
- Worry-Free Business Security Services

File Server and Storage

- Core Protection for Virtual Machines
- Deep Security
- PortalProtect for Sharepoint
- ServerProtect for EMC Celerra
- ServerProtect for Linux
- ServerProtect for Microsoft Windows/Novell NetWa
- ServerProtect for Network Appliance filers

FIGURE A-1. Trend Micro Technical Support site at downloadcenter.trendmicro.com

Knowledge Base

The Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do to. New solutions are added daily.

Also available in Knowledge Base are product FAQs, hot tips, preventive antivirus advice, and regional contact information for support and sales.

`http://esupport.trendmicro.com/`

And, if you can't find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question through an email message. Response time is typically 24 hours or less.

Sending Suspicious Code to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, visit the Trend Micro Submission Wizard URL:

`http://subwiz.trendmicro.com/SubWiz`

Click the “Submit a suspicious file/undetected virus” link.

You are prompted to supply the following information:

- **Email**: Your email address where you would like to receive a response from the antivirus team.
- **Product**: The product you are currently using. If you are using multiple Trend Micro products, select the product that has the most effect on the problem submitted, or the product that is most commonly in use.
- **Number of Infected Seats**: The number of users in your organization that are infected.
- **Upload File**: Trend Micro recommends that you create a password-protected zip file of the suspicious file, using the word “virus” as the password—then select the protected zip file in the **Upload File** field.
- **Description**: Please include a brief description of the symptoms you are experiencing. Our team of virus engineers “dissect” the file to identify and characterize any risks it might contain and return the cleaned file to you, usually within 48 hours.

Note: Submissions made through the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you click **Next**, an acknowledgement screen opens. This screen also displays a Tracking Number for the problem you submitted.

If you prefer to communicate by email, send a query to the following address:

`virusresponse@trendmicro.com`

In the United States, you can also call the following toll-free telephone number:

(877) TRENDAV, or 877-873-6328

TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide customers with up-to-the minute security information.

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging risks. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA.

Security Information Center

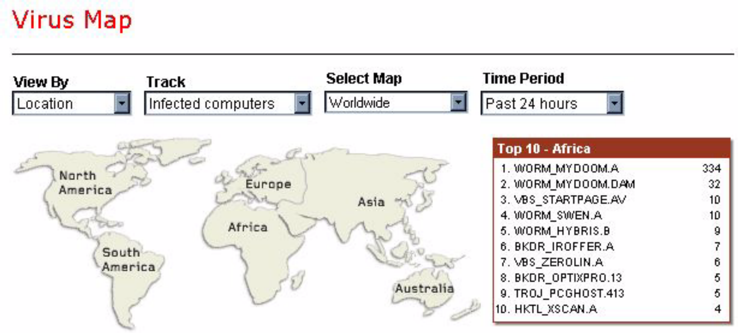
Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

`http://www.trendmicro.com/vinfo/`

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of risks expected to trigger in the current week, and describes the 10 most prevalent risks around the globe for the current week

- View a Virus Map of the top 10 risks around the globe



Virus Map

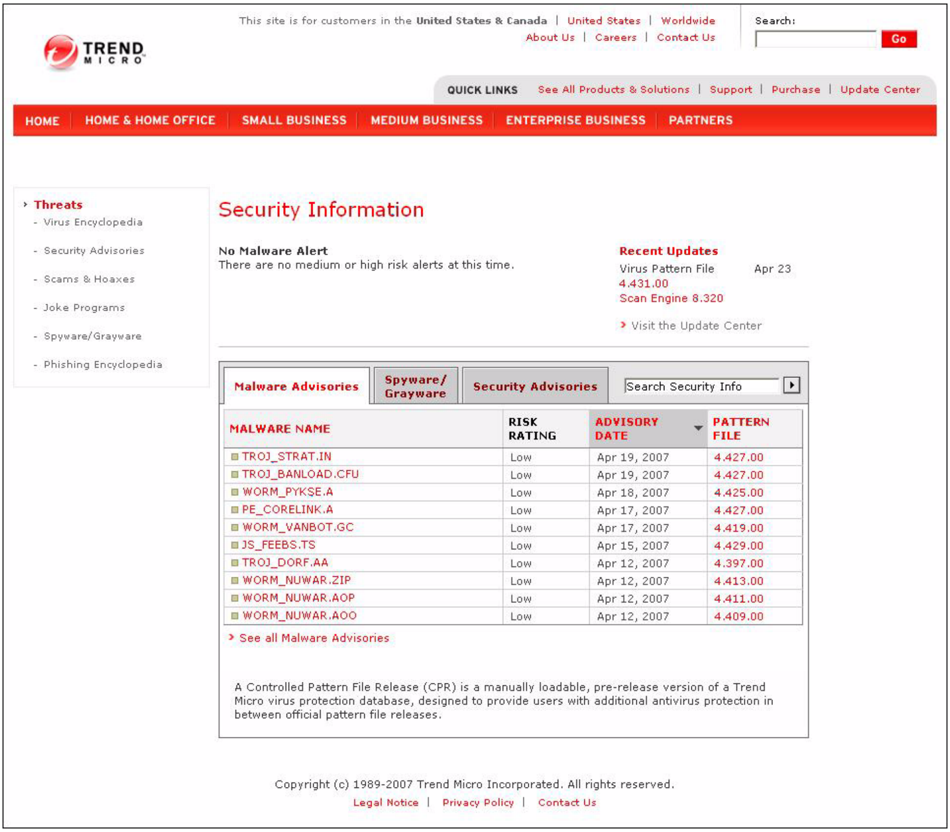
View By: Location
Track: Infected computers
Select Map: Worldwide
Time Period: Past 24 hours

Top 10 - Africa	
1. WORM_MYDOOM.A	334
2. WORM_MYDOOM.DAM	32
3. VBS_STARTPAGE.AV	10
4. WORM_SWEN.A	10
5. WORM_HYBRIS.B	9
6. BKDR_IROFFER.A	7
7. VBS_ZEROLIN.A	6
8. BKDR_OPTIXPRO.13	5
9. TROJ_PCGHOST.413	5
10. HKTL_XSCAN.A	4

FIGURE A-2. Trend Micro World Virus Tracking Program virus map

- Consult the Virus Encyclopedia, a compilation of known risks including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the risk, as well as information about computer hoaxes
- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:
  - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other risks
  - The Trend Micro *Safe Computing Guide*
  - A description of risk ratings to help you understand the damage potential for a risk rated Very Low or Low vs. Medium or High risk
  - A glossary of virus and other security risk terminology

- Download comprehensive industry white papers



This site is for customers in the **United States & Canada** | United States | Worldwide
About Us | Careers | Contact Us

Search: Go

TREND MICRO
QUICK LINKS
See All Products & Solutions | Support | Purchase | Update Center
HOME | HOME & HOME OFFICE | SMALL BUSINESS | MEDIUM BUSINESS | ENTERPRISE BUSINESS | PARTNERS
› Threats
- Virus Encyclopedia
- Security Advisories
- Scams & Hoaxes
- Joke Programs
- Spyware/Grayware
- Phishing Encyclopedia

Security Information

No Malware Alert
There are no medium or high risk alerts at this time.

Recent Updates
Virus Pattern File 4.431.00 Apr 23
Scan Engine 8.320

› Visit the Update Center

MALWARE NAME	RISK RATING	ADVISORY DATE	PATTERN FILE
TROJ_STRAT.IN	Low	Apr 19, 2007	4.427.00
TROJ_BANLOAD.CFU	Low	Apr 19, 2007	4.427.00
WORM_PYKSE.A	Low	Apr 18, 2007	4.425.00
PE_CORELINK.A	Low	Apr 17, 2007	4.427.00
WORM_VANBOT.GC	Low	Apr 17, 2007	4.419.00
JS_FEEBS.TS	Low	Apr 15, 2007	4.429.00
TROJ_DORF.AA	Low	Apr 12, 2007	4.397.00
WORM_NUWAR.ZIP	Low	Apr 12, 2007	4.413.00
WORM_NUWAR.AOP	Low	Apr 12, 2007	4.411.00
WORM_NUWAR.AOO	Low	Apr 12, 2007	4.409.00

› See all Malware Advisories

A Controlled Pattern File Release (CPR) is a manually loadable, pre-release version of a Trend Micro virus protection database, designed to provide users with additional antivirus protection in between official pattern file releases.

Copyright (c) 1989-2007 Trend Micro Incorporated. All rights reserved.
Legal Notice | Privacy Policy | Contact Us

FIGURE A-3. Trend Micro Security Information screen

- Subscribe, free, to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Webmasters

To open Security Information:

1. Open the IWSVA Web console.
2. Click **Security Info** from the drop-down menu at the top-right panel of the screen. The **Security Information** screen opens.

Appendix B

Mapping File Types to MIME Content-types

The following table describes some of the file types that you can enter in the HTTP and FTP virus scanning policy **MIME content-type to skip** field to skip scanning of the corresponding MIME content-types.

Overview

Potential MIME names are not limited to *Table B-1*, which means you can input any name into the IWSVA UI skip list. (See To select which file types to scan: on page 7-25 for details.) However, the MIME type can only be skipped under the following dependencies:

IWSVA receives a file and determines:

- Is the MIME name is set to be skipped on the UI
- Is the file type (not the MIME name) is listed in the mapping table:
- If the MIME name is in the mapping tables, is MIME name is on the UI skip list?

If IWSVA finds a match, it can be skipped. If IWSVA cannot find a match, it will not be skipped.

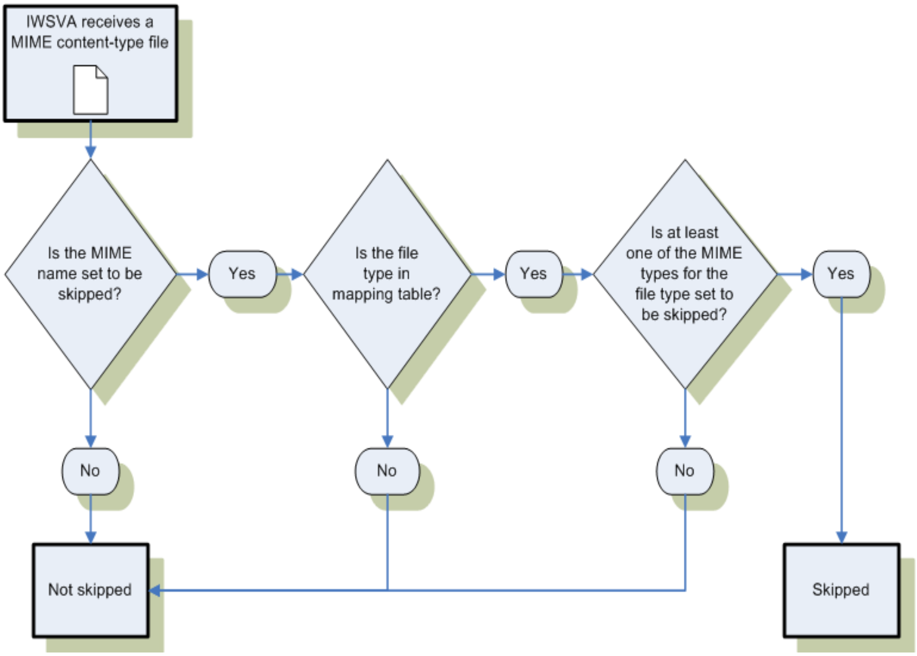

IWSVA receives a MIME content-type file
Is the MIME name set to be skipped?
Yes
Is the file type in mapping table?
Yes
Is at least one of the MIME types for the file type set to be skipped?
Yes
No
No
No
Not skipped
Skipped

FIGURE B-1. MIME Content Type Flow for Skipped Files

If an admin inputs a MIME name and the file type is unknown to IWSVA, IWSVA will skip the scanning of that file. If a MIME type is set to be skipped in IWSVA and it does not exist in the file type-MIME table, scanning will be skipped because the file type-MIME table can not list all possible MIME types for all possible file types.

If at least one of the MIME types for a file type is set to be skipped, it will also have scanning skipped because MIME names are not standard. The file type-MIME table can not list all MIME types for an known file type.

For example, the file type-MIME table contains mappings for FLV files: video/flv, video/x-flv: It does not contain "application/flv." However, some Web sites use "application/flv." IWSVA will not be able find the mapping entry for it, but IWSVA knows this is an FLV file by performing a file type check. It will skip the scan of this file.

If admin inputs "video/flv" and "application/flv" in skip list, the following check occurs:

- MIME name set to be skipped (MIME type: application/flv) >Yes >
- Check whether file type is in mapping table (file type: flv) > Yes >
- At least one of the MIME types for file type is set to skip >Yes > Skip the scan

File Type Mapping Table for MIME Content Files

TABLE B-1. File Type Mapping Table for MIME Content-Files

FILE TYPE	MIME CONTENT-TYPE
ACE Compression File	application/x-ace
ACE Compression File	application/x-compressed
Apple Sound	audio/aiff
Apple Sound	audio/x-aiff
Audio InterChange File Format from Apple/SGI	audio/aiff

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Audio InterChange File Format from Apple/SGI	audio/x-aiff
Audio InterChange File Format from Apple/SGI	sound/aiff
Audio InterChange File Format from Apple/SGI	audio/rmf
Audio InterChange File Format from Apple/SGI	audio/x-rmf
Audio InterChange File Format from Apple/SGI	audio/x-pn-aiff
Audio InterChange File Format from Apple/SGI	audio/x-gsm
Audio InterChange File Format from Apple/SGI	audio/x-midi
Audio InterChange File Format from Apple/SGI	audio/vnd.qcelp
ARJ	application/arj
ARJ	application/x-arj
ARJ	application/x-compress
ARJ	application/x-compressed
ARJ	zz-application/zz-winassoc-arj
Advanced Streaming Format	video/x-ms-asf
Advanced Streaming Format	video/x-ms-asf-plugin
Advanced Streaming Format	video/x-ms-wm

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Advanced Streaming Format	video/x-ms-wmx
Advanced Streaming Format	audio/asf
Advanced Streaming Format	application/asx
Advanced Streaming Format	application/x-mplayer2
Advanced Streaming Format	application/vnd.ms-as"
Nullsoft AVS	video/avs-video
Mime Base 64	application/base64
Macintosh MacBinary Archive	application/mac-binary
Macintosh MacBinary Archive	application/macbinary
Macintosh MacBinary Archive	application/octet-stream
Macintosh MacBinary Archive	application/x-binary
Macintosh MacBinary Archive	application/x-macbinary
BINHEX	application/binhex
BINHEX	application/binhex4
BINHEX	application/mac-binhex
BINHEX	application/mac-binhex40
BINHEX	application/x-binhex40
Windows BMP	image/bmp
Windows BMP	image/x-bmp
Windows BMP	image/x-bitmap

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Windows BMP	image/x-xbitmap
Windows BMP	image/x-win-bitmap
Windows BMP	image/x-windows-bmp
Windows BMP	image/ms-bmp
Windows BMP	image/x-ms-bmp
SGI Image	image/x-sgi-bw
GNU BZIP2	application/x-bzip2
GNU BZIP3	application/bzip2
GNU BZIP4	application/x-bz2
GNU BZIP5	application/x-compressed
Computer Graphics Metafiles	image/cgm
COM	application/octet-stream
COM	application/x-msdos-program
COM	application/x-msdownload
UNIX cpio Archive	application/x-cpio
Macromedia Director Shockwave Movie	application/x-director
WordPerfect	application/wordperfect
AutoCAD DWG	application/acad
AutoCAD DWG	application/x-acad

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
AutoCAD DWG	drawing/x-dwg
AutoCAD DWG	image/vnd.dwg
AutoCAD DWG	image/x-dwg
Encapsulated Postscript	application/postscript
Encapsulated Postscript	image/x-eps
Encapsulated Postscript	image/eps
Encapsulated Postscript	application/x-eps
Encapsulated Postscript	application/eps
EXE	application/octet-stream
EXE	application/exe
EXE	application/x-msdownload
EXE	application/x-exe
EXE	application/dos-exe
EXE	vms/exe
EXE	application/x-winexe
EXE	application/msdos-windows
Free Hand Document	image/x-freehand
AutoDesk Animator (FLI or FLC)	video/x-fli
AutoDesk Animator (FLI or FLC)	video/flc
AutoDesk Animator (FLI or FLC)	video/fli

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
AutoDesk Animator (FLI or FLC)	video/x-acad-anim
Macromedia Flash FLV Video	video/flv
Macromedia Flash FLV Video	video/x-flv
Macromedia Flash FLV Video	flv-application/octet-stream
Frame Maker	application/vnd.framemaker
GIF	image/gif
GNU ZIP	application/gzip
GNU ZIP	application/x-gzip
GNU ZIP	application/x-gunzip
GNU ZIP	application/gzipped
GNU ZIP	application/gzip-compressed
GNU ZIP	application/x-compressed
GNU ZIP	application/x-compress
GNU ZIP	gzip/document
GNU ZIP	encoding/x-gzip
Windows Icon	image/ico
Windows Icon	image/x-icon
Windows Icon	application/ico
Windows Icon	application/x-ico
Windows Icon	application/x-win-bitmap

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Windows Icon	image/x-win-bitmap
Amiga 8SVX Audio Interchange File Format	audio/x-aiff
Amiga 9SVX Audio Interchange File Format	image/iff
Amiga 10SVX Audio Interchange File Format	image/x-iff
Amiga 11SVX Audio Interchange File Format	application/iff
JAVA Applet	text/x-java-source
JAVA Applet	application/java-class
JAVA Applet	application/x-java-applet
JAVA Applet	application/x-java-vm
JPEG	image/jpeg
JPEG	image/jpg
JPEG	image/jp_
JPEG	image/pipeg
JPEG	image/pjpeg
LHA	application/x-lha
LHA	application/lha
LHA	application/x-compress
LHA	application/x-compressed

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
LHA	application/maclha
Compiled LISP	application/x-lisp
NT/95 Shortcut (*.lnk)	application/x-ms-shortcut
LightWave 3D Object	image/x-lwo
MAUD Sample Format	audio/x-maud
Microsoft Document Imaging	image/vnd.ms-modi
MIDI	audio/midi
Magick Image File Format	application/x-mif
Multi-image Network Graphics	video/x-mng
Multi-image Network Graphics	video/mng
MP3	audio/mpeg
MP3	audio/mpeg3
MP3	audio/x-mpeg-3
MPEG	video/mpeg
MPEG	video/mpg
MPEG	video/x-mpg
MPEG	video/mpeg2
MPEG	video/x-mpeg
MPEG	video/x-mpeg2a
Microsoft Cabinet	application/x-cainet-win32-x86

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Windows Word	application/msword
Windows Word	application/doc
Windows Word	application/vnd.msword
Windows Word	application/vnd.ms-word
Windows Word	application/x-msw6
Windows Word	application/x-msword
Windows Excel	application/excel
Windows Excel	application/x-msexcel
Windows Excel	application/x-ms-excel
Windows Excel	application/x-excel
Windows Excel	application/vnd.ms-excel
Windows Excel	application/xls
Windows Excel	application/x-xls
Windows Installer	application/x-ole-storage
Microsoft Access (MDB)	application/x-msaccess
Microsoft Access (MDB)	application/msaccess
Microsoft Access (MDB)	application/vnd.msaccess
Microsoft Access (MDB)	application/vnd.ms-access
Microsoft Access (MDB)	application/mdb
Microsoft Access (MDB)	application/x-mdb

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Microsoft Access (MDB)	zz-application/zz-winassoc-mdb
Microsoft Office 12	application/vnd.ms-word.document.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Microsoft Office 12	application/vnd.ms-word.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.wordprocessingml.template
Microsoft Office 12	application/vnd.ms-powerpoint.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.template
Microsoft Office 12	application/vnd.ms-powerpoint.addin.macroEnabled.12
Microsoft Office 12	application/vnd.ms-powerpoint.slideshow.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.slideshow
Microsoft Office 12	application/vnd.ms-powerpoint.presentation.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.presentation

Table B-1. File Type Mapping Table for MIME Content-Files (Continued)

File Type	MIME Content-type
Microsoft Office 12	application/vnd.ms-excel.addin.macroEnabled.12
Microsoft Office 12	application/vnd.ms-excel.sheet.binary.macroEnabled.12
Microsoft Office 12	application/vnd.ms-excel.sheet.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Microsoft Office 12	application/vnd.ms-excel.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.spreadsheetml.template
Microsoft Office 12	application/vnd.openxmlformats
Windows PowerPoint	application/mspowerpoint
Windows PowerPoint	application/powerpoint
Windows PowerPoint	application/vnd.ms-powerpoint
Windows PowerPoint	application/ms-powerpoint
Windows PowerPoint	application/mspowerpnt
Windows PowerPoint	application/vnd-mspowerpoint
Windows PowerPoint	application/x-powerpoint
Windows PowerPoint	application/x-mspowerpoint

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Windows Project	application/vnd.ms-project
Windows Project	application/x-msproject
Windows Project	application/x-project
Windows Project	application/msproj
Windows Project	application/msproject
Windows Project	application/x-ms-project
Windows Project	application/x-dos_ms_project
Windows Project	application/mpp
Windows Project	zz-application/zz-winassoc-mpp
Windows Write	application/mswrite
Windows Write	application/x-mswrite
Windows Write	application/wri
Windows Write	application/x-wri
Windows Write	application/msword
Windows Write	application/microsoft_word
Windows Write	zz-application/zz-winassoc-wri
Open Document	application/vnd.oasis.opendocument.text
Open Document	application/vnd.oasis.opendocument.text-template

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Open Document	application/vnd.oasis.opendocument.graphics
Open Document	application/vnd.oasis.opendocument.graphics-template
Open Document	application/vnd.oasis.opendocument.presentation
Open Document	application/vnd.oasis.opendocument.presentation-template
Open Document	application/vnd.oasis.opendocument.spreadsheet
Open Document	application/vnd.oasis.opendocument.spreadsheet-template
Open Document	application/vnd.oasis.opendocument.chart
Open Document	application/vnd.oasis.opendocument.chart-template
Open Document	application/vnd.oasis.opendocument.image
Open Document	application/vnd.oasis.opendocument.image-template
Open Document	application/vnd.oasis.opendocument.formula
Open Document	application/vnd.oasis.opendocument.formula-template
Open Document	application/vnd.oasis.opendocument.text-master

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Open Document	application/vnd.oasis.opendocument.text-web
Gravis Patch Files	audio/pat
Gravis Patch Files	audio/x-pat
Microsoft Paint v1.x	image/x-pcx
Microsoft Paint v1.x	image/pcx
Microsoft Paint v1.x	image/x-pc-paintbrush
Microsoft Paint v1.x	application/x-pcx
Microsoft Paint v1.x	application/pcx
Microsoft Paint v1.x	zz-application/zz-winassoc-pcx
Microsoft Paint v2.x	image/x-pcx
Microsoft Paint v2.x	image/pcx
Microsoft Paint v2.x	image/x-pc-paintbrush
Microsoft Paint v2.x	application/x-pcx
Microsoft Paint v2.x	application/pcx
Microsoft Paint v2.x	zz-application/zz-winassoc-pcx
PCX	image/x-pcx
PCX	image/pcx
PCX	image/x-pc-paintbrush
PCX	application/x-pcx

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
PCX	application/pcx
PCX	zz-application/zz-winassoc-pcx
Palm Pilot Image	application/x-pilot-pdb
Adobe Portable Document Format (PDF)	application/pdf
Adobe Portable Document Format (PDF)	application/x-pdf
Adobe Font File	application/x-font
Macintosh Bitmap	image/pict
Macintosh Bitmap	image/x-pict
Portable Network Graphics	image/png
PPM Image	image/x-portable-pixmap
PPM Image	image/x-p
PPM Image	image/x-ppm
PPM Image	application/ppm
PPM Image	application/x-ppm
Postscript	application/postscript
Adobe Photoshop (PSD)	application/octet-stream
Paint Shop Pro	image/bmp
Quick Time Media	video/quicktime
Quick Time Media	video/x-quicktime

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Quick Time Media	image/mov
Quick Time Media	audio/aiff
Quick Time Media	audio/x-midi
QuarkXPress Document (QXD)	application/quarkxpress
QuarkXPress Document (QXD)	application/x-quark-express
Real Audio	audio/vnd.rn-realaudio
Real Audio	audio/x-pn-realaudio
Real Audio	audio/x-realaudio
Real Audio	audio/x-pm-realaudio-plugin
Real Audio	video/x-pn-realvideo
RAR	application/rar
Sun Raster (RAS)	image/x-cmu-raster
Sun Raster (RAS)	image/cmu-raster
Real Media	application/vnd.rn-realmedia
Microsoft RTF	application/rtf
Microsoft RTF	application/x-rtf
Microsoft RTF	text/richtext
Lotus ScreenCam Movie	application/vnd.lotus-screencam
Lotus ScreenCam Movie	application/x-lotusscreencam
Lotus ScreenCam Movie	application/x-screencam

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Lotus ScreenCam Movie	video/x-scm
Lotus ScreenCam Movie	video/x-screencam
IRCAM Sound File	audio/x-sf
Sonic Foundry File	audio/sfr
Macromedia Flash	application/x-shockwave-flash
TAR	application/x-tar
TAR	application/tar
TAR	application/x-gtar
TAR	multipart/x-tar
TAR	application/x-compress
TAR	application/x-compressed
Targa Image	image/tga
Targa Image	image/x-tga
Targa Image	image/targa
Targa Image	image/x-targa
TIFF	image/tiff
TNEF file	application/ms-tnef
TNEF file	application/vnd.ms-tne
ASCII Text	text/plain
ASCII Text	application/txt

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
ASCII Text	text/html
ASCII Text	text/css
UUENCODE	text/x-uuencode
VBScript	text/vbscript
VBScript	text/vbs
VBScript	application/x-vbs
Creative Voice Format (VOC)	audio/voc
Creative Voice Format (VOC)	audio/x-voc
Microsoft RIFF	audio/wav
Microsoft RIFF	application/x-cdf
Microsoft RIFF	application/x-cmx
Microsoft RIFF	image/x-cmx
Microsoft RIFF	drawing/cmx
Microsoft RIFF	application/cmx
Webshots Picture Collection	application/x-webshots
Webshots Picture Collection	application/wbc
Windows Metafile	application/x-msmetafile
Windows Metafile	application/wmf
Windows Metafile	application/x-wmf
Windows Metafile	image/x-wmf

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Windows Metafile	zz-application/zz-winassoc-wmf
PKZIP	application/zip
PKZIP	application/x-zip
PKZIP	application/x-zip-compressed
PKZIP	multipart/x-zip
PKZIP	application/x-compress
PKZIP	application/x-compressed
ACE Compression File	application/x-ace
ACE Compression File	application/x-compressed
Apple Sound	audio/aiff
Apple Sound	audio/x-aiff
Audio InterChange File Format from Apple/SGI	audio/aiff
Audio InterChange File Format from Apple/SGI	audio/x-aiff
Audio InterChange File Format from Apple/SGI	sound/aiff
Audio InterChange File Format from Apple/SGI	audio/rmf
Audio InterChange File Format from Apple/SGI	audio/x-rmf
Audio InterChange File Format from Apple/SGI	audio/x-pn-aiff

TABLE B-1. File Type Mapping Table for MIME Content-Files (Continued)

FILE TYPE	MIME CONTENT-TYPE
Audio InterChange File Format from Apple/SGI	audio/x-gsm
Audio InterChange File Format from Apple/SGI	audio/x-midi
Audio InterChange File Format from Apple/SGI	audio/vnd.qcelp
ARJ	application/arj
ARJ	application/x-arj
ARJ	application/x-compress
ARJ	application/x-compressed
ARJ	zz-application/zz-winassoc-arj
Advanced Streaming Format	video/x-ms-asf
Advanced Streaming Format	video/x-ms-asf-plugin
Advanced Streaming Format	video/x-ms-wm
Advanced Streaming Format	video/x-ms-wmx
Advanced Streaming Format	audio/asf
Advanced Streaming Format	application/asx
Advanced Streaming Format	application/x-mplayer2

Appendix C

Architecture and Configuration Files

Topics in this appendix include the following:

Main Components

The following are the main InterScan Web Security Virtual Appliance (IWSVA) modules:

- **Main Program:** Installs the Web console and the basic library files necessary for IWSVA.
- **HTTP Scanning:** Installs the services necessary for HTTP scanning (either ICAP or HTTP scanning) and URL blocking.
- **FTP Scanning:** Installs the service that enables FTP scanning.
- **URL Filtering:** Installs the service necessary for URL filtering.
- **Applets and ActiveX Scanning:** Installs the service necessary for checking Java applet and ActiveX object digital signatures, and instrumenting applets so their execution can be monitored for prohibited operations.
- **SNMP Notifications:** Installs the service to send SNMP traps to SNMP-compliant network management software.
- **Control Manager Agent for IWSVA:** Installs the files necessary for the Control Manager agent to enable monitoring and configuration through Control Manager.

Main Services

To start or stop any of the services in this section, you must be logged on to IWSVA as `root` using either a local terminal or SSH. The root user can only stop or start the HTTP and FTP services from within IWSVA CLI (see Enabling the HTTP(s) Traffic Flow on page 5-2 and Enabling FTP Traffic and FTP Scanning on page 10-4). No other services can be stopped or started from within IWSVA.

The following services are used by IWSVA:

- **Trend Micro IWSVA Console (java):** This service is the Web server hosting the Web console.
- **Trend Micro IWSVA for FTP (isftpd):** This service enables the FTP traffic flow and FTP virus scanning.

- **Trend Micro IWSVA for HTTP (iwssd):** This service enables the HTTP traffic flow and HTTP scanning (including FTP over HTTP). It also handles Applets and ActiveX security processing.

Note: FTP over HTTP is not supported in Transparent Bridge Mode.

- **Trend Micro IWSVA Log Import (logtodb):** This service writes logs from text files to the database.
- **Trend Micro IWSVA Notification Delivery Service (isdelvd):** This service handles administrator notifications (through email) and user notifications (through browser).
- **Trend Micro SNMP Service (svcmonitor if using the Linux SNMP agent, snmpmonitor if using the IWSVA-installed SNMP agent):** This service sends SNMP trap notifications to SNMP-capable network monitoring devices.
- **Trend Micro Control Manager Service (En_Main):** This service permits IWSVA configuration and status reporting through Trend Micro Control Manager, if you are using Control Manager.
- **Trend Micro IWSVA for Dashboard (ismetricmgmtd):** This service collects system resource data to be used in the display of real-time dashboard metrics.

Scheduled Tasks

When installing IWSVA, the setup program creates several scheduled tasks.

- **purgefile:** Runs daily at 2:00 am to delete old text log files, subject to the configured time interval to retain logs.
- **schedulereport:** Runs hourly to check if a scheduled report is configured to run.
- **schedulepr_update:** Runs daily to check if it is time to update the product registration/license.
- **schedule_au:** Runs every 15 minutes to check if it is time to update the pattern file or other program components.
- **cleanfile:** Runs hourly, to remove temporary files downloaded for scan-behind or large file scanning.
- **DbOldDataCleanup.sh:** Runs daily at 2:05 am to clean up old reporting log data in the database and cleans up the old access quota counters in the database.

- **svc_snmpmonitor.sh:** Runs every 5 minutes to verify that the logtodb, mail, postgres and metric daemons are running. It restarts them if they are not.
- **db_reindex.sh:** Runs daily at 28 minutes past every other hour to rebuild corrupted database indices containing any invalid data. This maintains optimum database performance.
- **db_vacuum.sh:** Runs daily at 3:58 am to perform garbage collection to free up unused space from database tables in order to maintain optimum database performance.

About Configuration Files

To access configuration files, you must be logged on to the appliance as `root` using either a local terminal or SSH.

There are three types of configuration files: main, protocol module, and scanning module. All the configuration files are in the `{IWSS root}` directory; the default location for `{IWSS root}` is `/etc/iscan/`. The main configuration file is in `intscan.ini`.

- Settings specific to virus scanning are in:

  `{IWSS root}/IWSSPIScanVsapi.dsc`

- Settings that are specific to the ICAP protocol are in:

  `{IWSS root}/IWSSPIProtocolIcap.pni`

- Settings that are specific to the stand-alone proxy are in:

  `{IWSS root}/IWSSPIProtocolHttpProxy.pni`

- Settings for URL filtering scanning module are in:

  `{IWSS root}/IWSSPIUrlFilter.dsc`

- Settings specific to reporting are in:

  `{IWSS root}/report.ini`

- Settings for the URL Categorization database are in:

  `{IWSS root}/urlfxIFX.ini`

- Settings for default URL categories and their mapping information are in:

`{IWSS root}/urlfcMapping.ini`

- Settings for the list of IP address and IP ranges of all machines allowed to access the IWSVA device are in:

  `{IWSS root}/ClientACL_http.ini (for HTTP)`

  `{IWSS root}/ClientACL_ftp.ini (for FTP)`

- Settings for rules that define what ports IWSVA forwards HTTP requests to are in:

  `{IWSS root}/HttpPortPermission_http.ini (for HTTP)`

  `{IWSS root}/HttpPortPermission_ftp.ini (for FTP)`

- Settings for rules that define what ports IWSVA allows HTTPS tunneling to are in:

  `{IWSS root}/HttpsConectACL_http.ini`

- Settings for list of IP address and IP ranges of trusted servers are in:

  `{IWSS root}/ServerIPWhiteList_http.ini (for HTTP)`

  `{IWSS root}/ServerIPWhiteList_ftp.ini (for FTP)`

The IWSVA Web console varies depending on which modules are used. If you have been using a previous version of IWSVA, there are also many new features available in IWSVA that require new `.ini` file entries.

Protocol Handlers

Functions responsible for interpreting and processing messages in some recognized transmission protocols are encapsulated in a dynamic library referred to as a protocol handler. IWSVA provides a choice of either an ICAP protocol handler, which enables IWSVA to act as an ICAP server, or an HTTP proxy handler, wherein IWSVA acts like a direct HTTP proxy server. (The HTTP protocol handler is also used in bridge mode.) The application binary is independent of the protocol handler, allowing the same application to support different protocols with a configuration change.

Provide the complete path of the active configuration file of the protocol in the `main/protocol_config_path` entry in the `intscan.ini` file application.

Protocol handlers require their own specific configuration files, which contain entries that pertain only to that protocol. These protocol configuration files are denoted with a `.pni` filename extension.

Scanning Modules

Traffic scanning functionality is provided through dynamic libraries known as scanning modules. The first scanning module available to IWSVA provides content scanning using the scan engine.

Each scanning module has a configuration file with a `.dsc` extension. The IWSVA application locates the available scanning modules by searching for `.dsc` files in the directory that is provided in the `scan/plugin_dir` entry in the `intscan.ini` file.

Appendix D

OpenLDAP Reference

Though OpenLDAP supports Kerberos authentication, the packages to enable Kerberos authentication support are not installed by default. This appendix covers how to install and configure Kerberos support for OpenLDAP. In addition, this appendix explains how to set up your OpenLDAP directory so InterScan Web Security Virtual Appliance (IWSVA) can query it when using the user/group authentication method.

This chapter includes the following topics:

OpenLDAP Server Side Configuration

Software Package Dependencies

The following software packages are compatible with IWSVA:

- cyrus-sasl-2.1.19
- db-4.2.52.NC
- heimdal-0.6.2
- openldap-2.3.39
- openssl-0.9.7d

Configuration Files

Using OpenLDAP with IWSVA requires modifying the following configuration files:

```
/etc/openldap/ldap.conf

/etc/openldap/slapd.conf
```

Sample ldap.conf

```
#
# System-wide ldap configuration files. See ldap.conf(5) for
# details
# This file should be world readable but not world writable.


# OpenLDAP supports the ldap.conf file. You could use this file to
# specify a number of defaults for OpenLDAP clients. Normally this
# file can be found under /etc/openldap based on /etc/init.d/ldap
# start script's setting

# Set host IP address or fully qualified domain name

HOST example.peter.com
#HOST 10.2.1.1

# Set the default BASE DN where LDAP search will start off

BASE dc=peter,dc=com

# Set the default URI
```

```
URI ldap://example.peter.com

# SASL options
# specify the sasl mechanism to use. This is a user-only option.
# SASL_MECH <mechanism>
# specify the realm. This is a user-only option
# SASL_REALM <realm>
# specify the authentication identity.
# SASL_AUTHCID <authcid>
```

Sample slapd.conf

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
# Enforce all changes to follow the defined schemas loaded via
# include statements in the conf file


# NOTE 1
# All the OpenLDAP config files and backend databases are accessed
# and created by "ldap", so if you touch these config files by
# "root", "a Permission Denied" error will occur. Please modify
# ownership accordingly.

# NOTE 2
# krb5-kdc.schema fails to work with current OpenLDAP 2.2.x distro
# krb5ValidStart, krb5ValidEnd, krb5PasswordEnd need to have
# "EQUALITY generalizedTimeMatch" inserted before the ORDERING
# statement.
# www.openldap.org/lists/openldap-bugs/200309/msg00029.html

# Enforce all changes to follow the defined schemas loaded via
# include statements in the conf file

schemacheck on

# Included schemas

include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/krb5-kdc.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
include /usr/local/etc/openldap/schema/nis.schema
include /usr/local/etc/openldap/schema/java.schema
```

```
# Do not enable referrals because IWSVA 3.1 has its own implementation
# referral ldap://root.openldap.org

# Directives say where to write out slapd's PID and arguments
# started with

pidfile /usr/local/var/run/slapd.pid
argsfile /usr/local/var/run/slapd.args

# Load dynamic backend modules:
# modulepath/usr/local/libexec/openldap
# moduleloadback_bdb.la
# moduleloadback_ldap.la
# moduleloadback_ldbm.la
# moduleloadback_passwd.la
# moduleloadback_shell.la

# Sample security restrictions
#Require integrity protection (prevent hijacking)
#Require 112-bit (3DES or better) encryption for updates
#Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64

# Sample access control policy:
#Root DSE: allow anyone to read it
#Subschema (sub)entry DSE: allow anyone to read it
#Other DSEs:
#Allow self write access
#Allow authenticated users read access
#Allow anonymous users to authenticate
#Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
# access to *
#by self write
#by users read
#by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn. (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!
access to dn.base="" by * read
access to dn.base="cn=Subschema" by * read
access to *
```

```
by self write
by users read
by anonymous auth
by * none

# We have found this gives a useful amount of information about
# directory

loglevel 256

#Specify the number of threads used in slapd, default = 16
#Increasing or decreasing the number of threads used can
#drastically affect performance, we found 20 threads to be optimal
#for our setup, but it can be different under other operating
#systems

threads 20

#Tell slapd to close connections that have been idle for 30 seconds
#or more

idletimeout 30

# Enable LDAPv2 support. This option is disabled by default.

allow bind_v2

# Disable anonymous bind

disallow bind_anon

# Comment this section to enable simple bind

#disallow bind_simple

# NOTE 3
# SASL Configuration
# Caution: make sure you use the canonical name of the machine
# in sasl-host. Otherwise, OpenLDAP wont be able to offer GSSAPI
# authentication

# Set the SASL realm and canonical name of the host
sasl_hostexample.peter.com
sasl_realmPETER.COM

# Allow proxy authentication if it's configured

sasl-authz-policyboth

# NOTE 4
# Mapping of SASL authentication identities to LDAP entries
# The sasl-regexp line are particularly critical. They are what
# rewrite incoming connections who have SASL formatted DNs to the
# DNs that are in the directory DB. It's important to remember that
# they are processed in order, so you want to write them from most
# specific to most general

# NOTE 5
# We set the cn=.* since we are going to adopt different security
# mechanisms. If Kerberos v5 is the only one used, change wildcard
# to cn=GSSAPI,cn=auth

#sasl-regexp uid=(.*),cn=GSSAPI,cn=auth
#uid=$1,ou=people,dc=peter,dc=com

sasl-regexp uid=(.*),cn=.*,cn=auth uid=$1,ou=people,dc=peter,dc=com

# ldbm database definitions

# NOTE 6
# Correctly configuring the backend Berkeley DB is very critical
# follow the guideline at
# http://www.openldap.org/faq/data/cache/1073.html

# Cleartext passwords, especially for the rootdn, should
# be avoided. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.

databasebdb

# These options specify a DN and passwd that can be used to
# authenticate as the super-user entry of the database. The DN and
# password specified here will always work, regardless of whether
# the entry named actually exists or has the password given.
# This solves the chicken-and-egg problem of how to authenticate and
# add entries before any entries yet exist

suffix"dc=peter,dc=com"
rootdn"cn=admin,dc=peter,dc=com"
rootpwadmin

# NOTE 7
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700
# recommended.

directory/usr/local/var/openldap-data

#Tell the slapd to store the 10000 most accessed entries in memory
#Having a properly configured cache size can drastically affect
#performance
```

```
cachesize 10000

# Indices to maintain
# Some versions of OpenLDAP don't support the index of uniqueMember
# "pres" indexing allows you to see a filter that asks if the
# attribute is present in an entry
# "eq" indexing allows to ask if an attribute has an exact value
# "apporx" indexing allows to ask if an attribute value sounds like
# something
# This option is tied to --enable-phonetic compile option in
# OpenLDAP
# "sub" indexing allows to do substring search on an attribute's
# values

index default eq,pres
index objectclass  eq,pres
index cn,sn,givenname,mail   eq,pres,approx,sub
index uideq,pres
index uidNumber,gidNumber,memberUid   eq,pres
```

Tools

To create the server database and associate indices by importing an existing LDIF file:

NAME

slapadd - Add entries to a SLAPD database

SYNOPSIS

```
/usr/sbin/slapadd  [-v]  [-c]  [-d  level] [-b suffix] [-n dbnum]
[-f slapd.conf] [-l ldif-file]
```

DESCRIPTION

Slapadd is used to add entries specified in LDAP Directory Interchange Format (LDIF) to a slapd database.

- Dump the server database to an LDIF file. This can be useful when you want to make human-readable backup of current database.

NAME

slapcat - SLAPD database to LDIF utility

SYNOPSIS

```
/usr/sbin/slapcat  [-v]  [-c]  [-d  level] [-b suffix] [-n dbnum]
[-f slapd.conf] [-l ldif-file]
```

DESCRIPTION

slapcat is used to generate an LDAP Directory Interchange Format (LDIF) output based upon the contents of a slapd database.

- Rebuilds all indices based upon the current database contents

NAME

slapindex - SLAPD index to LDIF utility

SYNOPSIS

```
/usr/sbin/slapindex [-f slapd.conf] [-d level] [-b suffix] [-n
dbnum]
```

DESCRIPTION

Slapindex is used to regenerate slapd indices based upon the current contents of a database.

- Check the settings of slapd.conf

NAME

Slaptest – Check the suitability of the slapd conf file

SYNOPSIS

```
/usr/sbin/slaptest  [-v]  [-d  level] [-f slapd.conf]
```

DESCRIPTION

Slaptest is used to check the conformance of the slapd.conf configuration file. It opens the slapd.conf configuration file, and parses it according to the general and the backend-specific rules, checking its conformance.

- LDAP query utility

NAME

ldapsearch - LDAP search tool

SYNOPSIS

```
ldapsearch  [-D binddn] [-W]  [-w bindpasswd] [-H ldapuri] [-h
ldaphost] [-p ldap- port]  [-b searchbase] [-s base|one|sub] [-x]
[-Y mech] [-Z[Z]] filter [attrs...]
```

DESCRIPTION

ldapsearch opens a connection to an LDAP server, binds, and performs a search using specified parameters.

EXAMPLE

The command performs a query using simple plain text authentication for a matched entry with “uid=petery” and requests the mail attribute for a matched entry to be returned by the LDAP server.

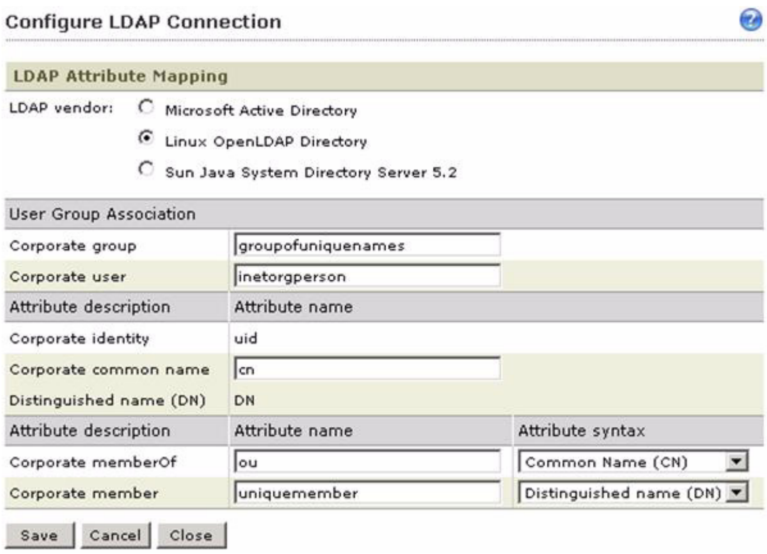
```
ldapsearch -x -D "cn=admin,dc=peter,dc=com" -w admin -b
"dc=peter,dc=com" -s sub "uid=petery" mail
```

For further information, consult the manual page.

```
Verify SASL/OpenLDAP/Kerberos v5 Authentication

1. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapsearch -v -x \

-D "cn=admin,dc=peter,dc=com" -W -b "" -s base -LLL \

-H ldap://example.peter.com/ supportedSASLMechanisms

2. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapsearch -b
"dc=peter,dc=com" \

-H ldap://example.peter.com/

3. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapwhoami -H
ldap://example.peter.com
```

Customized Attribute Equivalence Table Configuration

If you configure IWSVA to use the OpenLDAP or Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server) directories, there are several user group associations that can be configured.



Configure LDAP Connection

LDAP Attribute Mapping

LDAP vendor:
○ Microsoft Active Directory
● Linux OpenLDAP Directory
○ Sun Java System Directory Server 5.2

User Group Association

Corporate group	groupofuniquenames	
Corporate user	inetorgperson	
Attribute description	Attribute name	
Corporate identity	uid	
Corporate common name	cn	
Distinguished name (DN)	DN	
Attribute description	Attribute name	Attribute syntax
Corporate memberOf	ou	Common Name (CN)
Corporate member	uniquemember	Distinguished name (DN)

FIGURE D-1. OpenLDAP attribute mapping configuration screen

The **Corporate group** field tells IWSVA the object class to use as part of the LDAP search filter when searching for LDAP group objects. The "Corporate user" indicates the object class to use as part of the search filter for user objects. Because LDAP cannot distinguish whether an entry is group or user-specific, IWSVA needs this "tag" to perform the query.

The **Corporate memberOf** field defines the group membership of an entry, a user or a group while the "Corporate member" field specifies the members in a group entry because a user is the finest entity and cannot contain any member. An attribute name is the first column in this equivalence table and it specifies the attribute that contains relevant information. Default attributes are "ou" and "uniquemember" in the standard OpenLDAP schema.

Attribute syntax is the second column in the equivalence table and it defines the attribute that IWSVA needs to associate and look up to locate the group or member entry in the LDAP server. IWSVA provides two options to configure this setting, namely {"Common Name (CN)", "Distinguished Name (DN)}.

Consider the following simple LDIF file as an example, keeping in mind the following:

- LDIF is a method for representing data in an LDAP directory in a human readable format.
- To simplify the example, some entries have been removed.
- To dump a LDIF file of an OpenLDAP server, execute slapcat, usually under the OpenLDAP installation path or `/usr/local/sbin`.

  ```
  slapcat -l [output_file_name]
  ```

LDIF Format Sample Entries

See the following simplified example of a user entry in LDIF format.

EXAMPLE:

```
dn: uid=peterx,ou=People,dc=client,dc=us,dc=Xnet,dc=org
givenName: Peter
telephoneNumber: +1 408 555 5555
sn: Peter
ou: All of IWSVA Developer Team
ou: People#Corporate User field
mail: peterx@peter.com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: peterx
cn: Peter X
```

See the following simplified example of a group entry in LDIF format.

EXAMPLE:

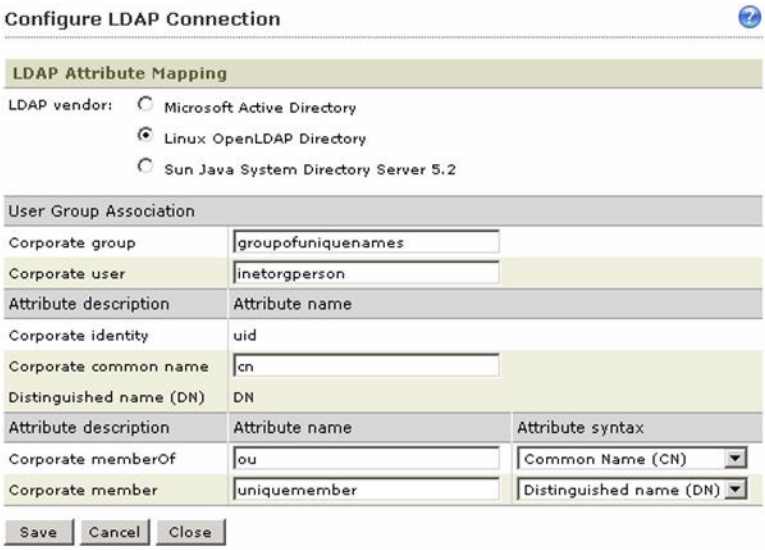
```
dn: cn=All of IWSVA Developer

Team,ou=Engineering,ou=Groups,dc=client,dc=us,dc=Xnet,dc=org
ou: Groups #Corporate Group field
ou: Engineering
description: All of IWSVA Developer Team
objectClass: top
objectClass: groupOfUniqueNames
uniqueMember:uid=peterx,ou=People,dc=client,dc=us,dc=Xnet,dc=org
cn: All of IWSVA Developer Team
```

Note the following:

- Associate the "Corporate Member" between a group and user entry using "Distinguished Name (DN)" as the attribute syntax.
- Associate the "Corporate MemberOf" in a group and user entry using "Common Name (CN)" as the attribute syntax.

Sample Configuration

Consider the following LDAP attribute mapping:



Configure LDAP Connection

LDAP Attribute Mapping

LDAP vendor:
○ Microsoft Active Directory
● Linux OpenLDAP Directory
○ Sun Java System Directory Server 5.2

User Group Association		
Corporate group	groupofuniquenames	
Corporate user	inetorgperson	
Attribute description	Attribute name	
Corporate identity	uid	
Corporate common name	cn	
Distinguished name (DN)	DN	
Attribute description	Attribute name	Attribute syntax
Corporate memberOf	ou	Common Name (CN)
Corporate member	uniquemember	Distinguished name (DN)

FIGURE D-2. OpenLDAP attribute mapping configuration screen

See the following sample user entry in LDIF format.

EXAMPLE:

```
dn: uid=peterx,ou=People,dc=client,dc=us,dc=Xnet,dc=org
givenName: Peter
telephoneNumber: +1 408 555 5555
sn: Peter
ou: All of Developer Team
ou: Employee#Corporate User field
mail: peterx@peter.com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

```
uid: peterx
cn: Peter X
```

See the following sample group entry in LDIF format.

EXAMPLE:

```
dn: cn=All of Developer
Team,ou=Engineering,ou=Groups,dc=client,dc=us,dc=Xnet,dc=org
ou: Teams #Corporate Group field
ou: Engineering
description: All of Developer Team
objectClass: top
objectClass: groupOfUniqueNames
teamMember: Peter X
cn: All of Developer Team
```

Note the following:

1. Associate the "Corporate Member" between a group and user entry using "Distinguished Name (DN)" as the attribute syntax.
2. Associate the "Corporate MemberOf" in a group and user entry using "Common Name (CN)" as the attribute syntax.

Appendix E

Best Practices for IWSVA

This appendix contains information about the best practices to follow for InterScan Web Security Virtual Appliance.

The topics include:

Authenticating Multiple Users on Shared Personal Computers

Supporting multiple users on a single shared personal computer (PC) using Microsoft Active Directory server for authentication can present some challenges to IT managers and users alike. IWSVA provides authentication based on a browser challenge and can support the authentication of multiple users on a shared PC using Microsoft Internet Explorer as the default browser.

Best Practice Suggestions

Leveraging Microsoft ShellRunas Utility

- For shared PCs, you can leverage the Microsoft ShellRunas utility to force the user to authenticate each time Microsoft Internet Explorer is started. The AD credentials are used to authenticate the user and Internet Explorer will leverage the credentials to automatically populate the user ID information in the HTTP header to allow IWSVA to identify the user for logging, reporting, and policy enforcement purposes.
- Download the MS ShellRunas utility from:

  http://technet.microsoft.com/en-us/sysinternals/cc300361.aspx
- Users must remember to shut down their IE browser sessions when they're finished using the computer. This allows Microsoft Internet Explorer to prompt the next user for their credentials. User education is critical to the success of this tool.
- Optionally, you can also modify the IP User Cache parameter to extend or shorten the cache interval for the authenticated user cache to further fine tune when users should be prompted for their authentication credentials. The default IWSVA user cache value is 1.5 hours (90 minutes). See the "`configure module ldap ipuser_cache interval <interval>`" CLI command for more information.

Scanning Considerations

IWSVA's malware scanning architecture is a hybrid solution that uses cloud-based malware detection methods such as Trend Micro's Smart Protection Network (SPN) and local, on-box scan technologies and signature files.

Smart Protection Network - Cloud Based Services

IWSVA's Smart Protection Network (SPN) is the industry's highest performing cloud-based malware protection service. Smart Protection Network has the following malware detection components:

- **Web Reputation Services (WRS)** is comprised of several correlated services that provide proactive detection and blocking against known bad web sites, domains, files and objects, as well as email related items - including anti-pharming and anti-phishing detection.
  - Domain reputation
  - Page reputation
  - Email reputation
  - File reputation
- **URL Filtering Service** stores its URL database in the cloud for rapid updates and protects Trend Micro's global user base without the need to download and update URL database files on the IWSVA server. This provides up-to-date URL information to every customer and accelerates the proactive protection capabilities to reduce the time between the discovery of a bad site and the time it is added to the URL database to protect all customers.
- **Feedback Loop** provides real-time information from all of Trend Micro's products to update the SPN cloud-based components and URL filtering databases. Malware detected on customer premise equipment are fed back into the cloud architecture and used to fine-tune information in real time. This provides fast proactive protection with low false positives to Trend Micro’s global customer base.

Best Practice Suggestions

Smart Protection Network (SPN) uses cloud-based services and relies on DNS queries for lookups. In order to ensure fast response and minimum latency, the IWSVA device must be configured with a primary and a secondary DNS server.

The DNS servers must be able to support the volume of DNS requests made by IWSVA. In general, before IWSVA builds up its local DNS cache, two DNS requests will be made for each URL accessed. Make sure your DNS server is installed on a server with enough resources and performance to handle the extra DNS volume.

Your DNS server should have a fast network card and be installed on a fast network switch to reduce latency.

Trend Micro recommends on-site DNS servers versus ISP provided DNS servers that are housed outside of the company's network. In general, ISP DNS servers have higher latency and do not support large numbers of DNS queries from a single IP address. Many ISP DNS servers have throttling mechanisms that limit the number of DNS requests per second and can affect IWSVA's Web Reputation Services (WRS) performance.

Try to place your DNS server as close to the IWSVA unit(s) as possible to eliminate unnecessary network hops between the devices to improve network response time and performance.

WRS and URL Filtering requests are made over HTTP port 80. Do not block the IWSVA management IP address for these ports on your firewall.

Local IWSVA Scan Engines

IWSVA provides local on-box scanning to ensure that content downloaded from the Internet is scanned for malware. Smart Protection Network's Web Reputation Service and URL Filtering services can filter a large percentage of the well-known and newly discovered malware sites and content, but local file scanning ensures that files and objects received are free of embedded viruses, worms, and other malicious code such as Trojans.

IWSVA provides the following local scan engines:

- **WRS Page Analysis** provides real-time content scanning with automatic update service to the Smart Protection Network to ensure that no zero-day threats are found on web sites with good reputation ratings. Any malware found triggers an automated update to the Smart Protection Network to re-examine the source of the content and to update its reputation score.
- **File Type Block** provides the ability to identify and block over 60 different file MIME types. These can include popular files such as Java applets, executable files, Microsoft Office documents, and so forth. See Mapping File Types to MIME Content-types on page B-1 for a detailed list of the supported file type.
- **IntelliTunnel** provides the ability to detect and block popular Instant Messaging applications.

- **Virus Scan (VSAPI)** provides signature based virus and malware scanning.
- **IntelliScan** provides the ability to identify and scan files based on their true file type, preventing users from trying to bypass the scan engines by changing the file extension or by some other form of file manipulation.
- **IntelliTrap** provides heuristics scanning to identify and protect against malware that changes or morphs from one state to another as it navigates through the network.
- **Compressed File Scanning** provides protection against malware that is hidden in highly-compressed files that are compressed many times over. Malware authors use this common delivery method to try and evade traditional anti-virus scanning software.
- **Spyware/Grayware Scanning** protects against spyware, dialers, hacking tools, password cracking applications, adware, joke programs, remote access tools, and other grayware types. This local scan engine provides protection based on spyware signatures and is used to compliment the Spyware URL category found in the URL Filtering feature. The local Spyware/Grayware scan engine is used to scan against files download or uploaded to the Internet that may be infected with spyware or grayware. Whereas the URL Filtering Spyware category is used to proactively block access to sites known to contain spyware related files and objects.
- **Applets and ActiveX Scanning** provides protection from malware embedded in Java applets and mobile code such as ActiveX applications found on many modern web sites.
- **Large File Scanning** provides administrators with a way to bypass scanning for large files that can consume a lot of system resources. Traditionally, malware authors do not embed viruses in large files because they want the malware to spread quickly without drawing a lot of attention to the file.

Best Practice Suggestions

- IWSVA's local scan services operate in a specific order to reduce the need to scan unnecessarily. IWSVA's scanning order for Internet traffic flows in the following order starting with the proactive Smart Protection Network's cloud-based services first.
    - Web Reputation Service (WRS)
    - URL Filtering Service
    - IntelliTunnel

  - File Type Block
  - Virus Scan
  - IntelliTrap Heuristics
  - MacroTrap
  - IntelliScan True File Type
  - Applets and ActiveX
- The Virus Scan (VSAPI) scan engine consumes the most resources. Enabling Web Reputation (WRS) and subscribing to the URL Filtering service and enabling its Computer/Harmful category can greatly reduce the need to perform traditional VSAPI-based virus scans. Making these changes can reduce server resources and provide additional scalability for your environment.
- For trusted, white-listed sites and files that have a high integrity rating, you can disable malware scanning to improve performance and reduce server resource use. Use the Global Trusted URLs, Approved URL and Approved File white lists in the Exception tabs to bypass scanning for trusted sites and files.
- You can configure large file scanning to skip scanning for files over a specific size. This can help reduce unnecessary scanning for larger files and lower resource use to improve capacity and performance.
- To improve user response time for larger file downloads, enable the Large File Handling's Deferred Scanning feature to “trickle” parts of the scanned file to the requesting host. This keeps the browser's file transfer status indicator alive and shows progress to the user while the file is scanned. If malware is found within the trickled file, IWSVA blocks the remainder of the file - resulting in an incomplete file that cannot be executed. For multi-media files or streaming content that uses HTTP port 80, such as YouTube content, you must enable Deferred Scanning to allow portions of the media to flow through. Selecting the “Scan Before Delivery” option blocks the streaming content until it is fully scanned and results in bad user experiences.
- For customers that need to scan the entire file before delivering it to their users, select the “Scan Before Delivery” option from the Large File Handling feature. This instructs IWSVA to buffer the file and completely scan it before delivering any portion to the user. This method is slightly slower in terms of end-user performance perception, but ensures that no portion of the infected file is allowed through.

- Keep in mind that entries placed in the Global Trusted URLs white list are not scanned. If you want to scan white listed items, create an Approved List object and use this in the policy's Exception tab. The Exception Tab gives you the option of scanning white listed items in the HTTP and FTP Scan Policies.

Transparent Identification Topology

Figure E-1 shows the typical transparent bridge mode network topology used when deploying IWSVA with transparent identification in your organization.

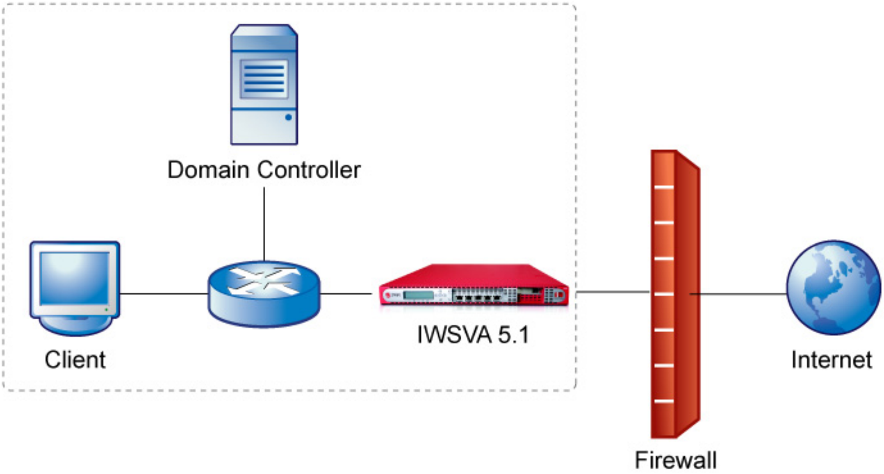


FIGURE E-1. Typical transparent bridge mode network topology used when deploying IWSVA with Transparent Identification

In *Figure E-1*, IWSVA sits behind the firewall with access to the Domain Controllers and client machines, required for Transparent Identification. If there is a NAT or firewall between client machines or Domain Controllers and IWSVA, the Transparent Identification query might fail.

In your organization, if the domain structure is not a single domain, but a tree or a forest, Trend Micro recommends that you enable the Global Catalog in the Domain Controller used by IWSVA as shown in *Figure E-1*. It not only reduces the logon traffic passing through the Internet and saves your bandwidth, but it also speeds up the log on process and helps IWSVA to obtain user/group information more quickly.

Transparent Identification Settings

Before starting the next procedure, check the following:

- **Domain Controller Settings:** Create a new account or use an existing one that belongs to 'Domain Admins' group in your Domain Controller for IWSVA used to query for user/group information.
- **Client Settings:** Configure the 'Windows Management Instrumentation (WMI) to start automatically and verify it is started on the clients.
- **Firewall Settings:** Verify the Windows firewall or other personal firewall in the client or the Domain Controller allows WMI traffic to pass.

  If you use Windows firewall in your client machines, you can deploy a group policy to change the default firewall settings in each client machine joined to the domain. This will automate the client configuration procedure and simplify deployment. See the following procedures for more information:

  - To create a group policy object: on page E-9
  - To apply the new Group Policy Object to all client machines: on page E-10

Step 1. Creating the Group Policy Object and Linking It to the Proper Organizational Unit

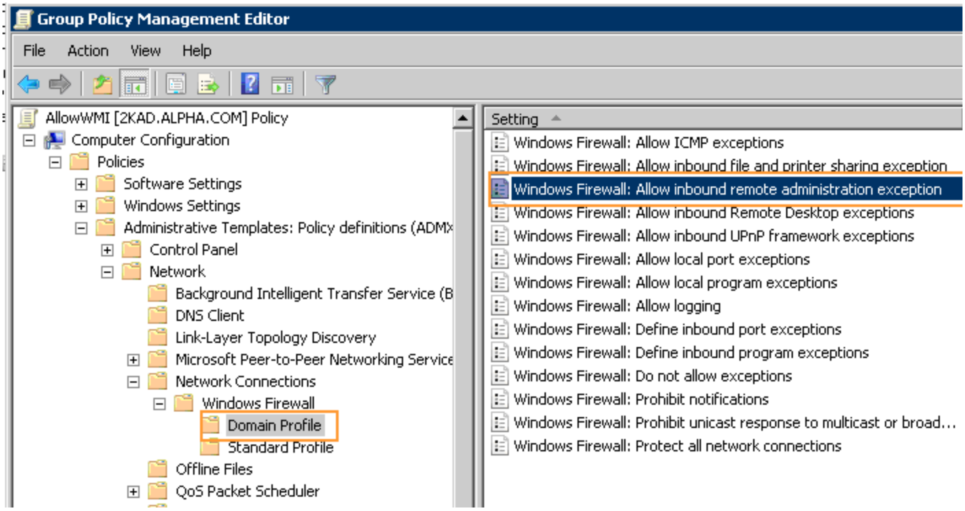

Group Policy Management Editor
File
Action
View
Help
AllowWMI [2KAD.ALPHA.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (ADMX
Control Panel
Network
Background Intelligent Transfer Service (B
DNS Client
Link-Layer Topology Discovery
Microsoft Peer-to-Peer Networking Service
Network Connections
Windows Firewall
Domain Profile
Standard Profile
Offline Files
QoS Packet Scheduler
Setting
Windows Firewall: Allow ICMP exceptions
Windows Firewall: Allow inbound file and printer sharing exception
Windows Firewall: Allow inbound remote administration exception
Windows Firewall: Allow inbound Remote Desktop exceptions
Windows Firewall: Allow inbound UPnP framework exceptions
Windows Firewall: Allow local port exceptions
Windows Firewall: Allow local program exceptions
Windows Firewall: Allow logging
Windows Firewall: Define inbound port exceptions
Windows Firewall: Define inbound program exceptions
Windows Firewall: Do not allow exceptions
Windows Firewall: Prohibit notifications
Windows Firewall: Prohibit unicast response to multicast or broad…
Windows Firewall: Protect all network connections

FIGURE E-2. Allow inbound remote administration exception

To create a group policy object:

1. Go to the Group Management Policy editor.
2. Go to **Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Windows Firewall**.
3. Double-click **Domain Profile**.
4. Click **Windows Firewall: Allow remote administration exception**.
5. On the Action menu, select **Properties**.
6. Click **Enable**, and then click **OK**.

Step 2. Applying the Group Policy Object to all client machines

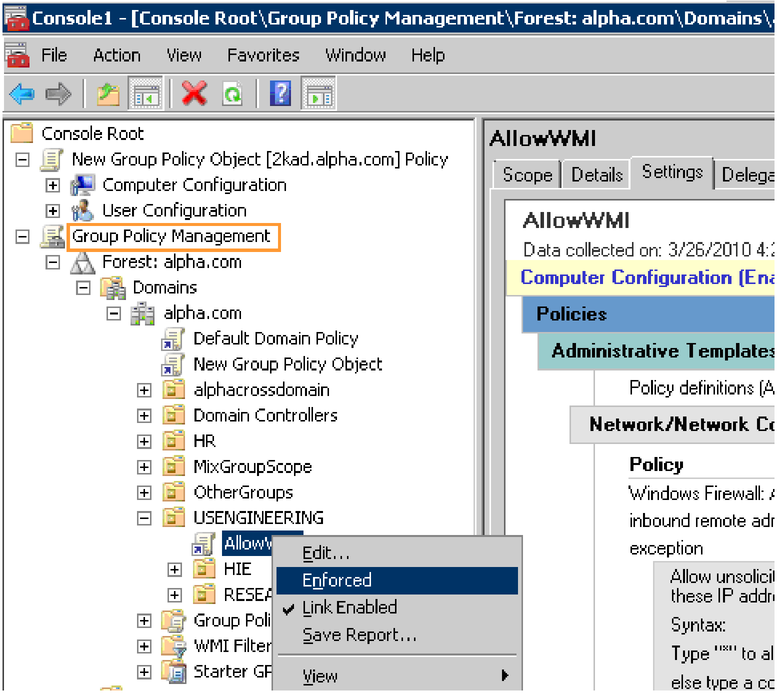


FIGURE E-3. **Enforce the Group Policy Object to all clients in the organizational unit**

To apply the new Group Policy Object to all client machines:

1. Go to the Group Policy Management MMC snap-in. (See *Figure E-3*.)
2. Right-click the newly added **Group Policy Object**.
3. Select **Enforced**.

Configuring Transparent Identification

Before starting this procedure, IWSVA should be configured with a valid DNS server that has good performance for resolving DNS requests. Make sure IWSVA can resolve the Domain Controller's hostname in the DNS server.

To configure Transparent Identification in IWSVA:

1. Select the **HTTP > Configuration > User Identification | User Identification** tab from the main menu.
2. Under the User Identification Method section, check **User/group name authorization**.
3. Under the User/group Authentication Settings section in the LDAP Settings section, click the **Select LDAP vendor** link.
4. In the secondary browser window, select **Microsoft Active Directory** from the list of supported the LDAP vendors
5. In the Configure LDAP Connection secondary window, click **Save** to confirm your LDAP vendor choice.
6. On the User Identification configuration screen, in the LDAP Settings section, type the **LDAP server host name** using the Fully Qualified Domain Name (FQDN).

   Note: Entering the LDAP server hostname's IP address is also acceptable, but FQDN format is recommended due to an incompatibility between Kerberos servers and identifying LDAP servers using their IP address.

7. Type the **Listening port number** used by the LDAP server that you have chosen (Default = 389).

   Note: If you have enabled the Global Catalog (GC) port as recommended, change the listening port to 3268.

8. Type the **Admin account** and **password** of the new created or existing account of “Domain Admins” group.

   You should use the UserPrincipalName for the admin account in the following format: NT_logon_ID@domain. For example: chris@trendmicro.com
9. Type the **Base distinguished name** to specify which level of the directory tree IWSVA should begin LDAP searches.

   The base Domain Name is derived from the company's DNS domain components; for example, LDAP server us.example.com would be entered as DC=example, DC=com.

10. Select the LDAP authentication method to use **Advanced (Kerberos Authentication)**.
11. Additionally, configure the following parameters to use Advanced authentication: (By default, the following setting will be automatically filled in, when enter 'Tab' button)
    - Default realm
    - Default domain
    - KDC and Admin Server: the same host name as your Active Directory server.
    - KDC Port Number: Default port = 88
12. Click the check boxes for **Enable Windows client query** and **Enable Domain Controller query** to enable both.
13. Click the Test Client link to test the client connection. It should be successful.

    Clicking the check box for Enable Domain Controller query allows IWSVA to receive the event logs for the Domain Controllers listed and to parse the event logs for user information.

    When the "Enable Domain Controller query" is first enabled, users receive a prompt to add the Domain Controller server(s) or to refresh the list of Domain Controller servers. Do the following:

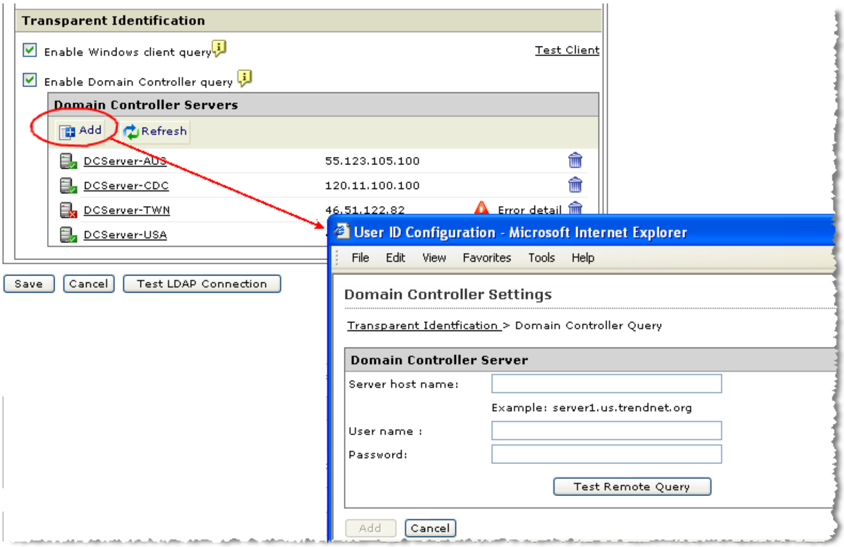
    a. Click **Refresh** to auto-detect Domain Controller servers.

    b. If new Domain Controller servers are not auto-detected, add them manually by clicking **Add**. (See *Figure E-4*.)

    c. Type the Domain Controller information in the secondary window, and click **Test Remote Query** to verify the Domain Controller server connection.

       All Domain Controller servers added to the configuration file allow IWSVA to query the event logs for username and IP address information.

    d. Make sure the status of all Domain Controllers in the list is OK as indicated by the small green check mark before going to next step.



Transparent Identification

☑ Enable Windows client query

☑ Enable Domain Controller query

Domain Controller Servers

DCServer-AUS	55.123.105.100	
DCServer-CDC	120.11.100.100	
DCServer-TWN	46.51.122.82	Error detail
DCServer-USA		

User ID Configuration - Microsoft Internet Explorer

Domain Controller Settings

Transparent Identfication > Domain Controller Query

Domain Controller Server

Server host name:

Example: server1.us.trendnet.org

User name :

Password:

FIGURE E-4. Enter Domain Controller information and text the remote query

14. If necessary, add information for the additional LDAP servers.

Note: All Active Directory domain controllers used to authenticate users to the domain should be added to the LDAP server list.

15. To verify the information has been entered correctly and IWSVA can communicate with the LDAP servers that you configured, click **Test LDAP Connection** on the User Identification page.

    A message box appears, indicating that you have successfully contacted the LDAP server.

16. Click **Save**.

Glossary of Terms

This glossary describes special terms as used in this document or the online help.

TERM	EXPLANATION
100BaseT	An alternate term for “fast Ethernet,” an upgraded standard for connecting computers into a local area network (LAN). 100BaseT Ethernet can transfer data at a peak rate of 100 Mbps. It is also more expensive and less common than 10BaseT. *Also see* 10BaseT.
10BaseT	The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable. Ethernet is a standard for connecting computers into a local area network (LAN). The maximum cable distance is 100 meters (325 feet), the maximum devices per segment is 1, and the maximum devices per network are 1024. *Also see* 100BaseT.
access (verb)	To read data from or write data to a storage device, such as a computer or server.
access (noun)	Authorization to read or write data. Most operating systems allow you to define different levels of access, depending on job responsibilities.

TERM	EXPLANATION
action (*Also see* target and notification)	The operation to be performed when: - a virus has been detected - spam has been detected - a content violation has occurred - an attempt was made to access a blocked URL, or - file blocking has been triggered. Actions typically include clean and deliver, quarantine, delete, or deliver/transfer anyway. Delivering/transferring anyway is not recommended—delivering a virus-infected message or transferring a virus-infected file can compromise your network.
activate	To enable your software after completion of the registration process. Trend Micro products are not operable until product activation is complete. Activate during installation or after installation (in the Web console) on the Product License screen.
Activation Code	A 37-character code, including hyphens, that is used to activate Trend Micro products. Here is an example of an Activation Code: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 *Also see* Registration Key.
active FTP	Configuration of FTP protocol that allows the client to initiate "handshaking" signals for the command session, but the host initiates the data session.
active/passive pair	A cluster composed of two machines contains one machine is active for traffic scan, while the other machine is passive and does not scan traffic. The passive device works as backup of to the active device to meet high availability requirements.

TERM **EXPLANATION**

ActiveUpdate

ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files through the Internet or the Trend Micro Total Solution CD or DVD.

ActiveX

A type of open software architecture that implements object linking and embedding, enabling some of the standard interfaces, such as downloading of Web pages.

ActiveX malicious code

An ActiveX control is a component object embedded in a Web page which runs automatically when the page is viewed. ActiveX controls allow Web developers to create interactive, dynamic Web pages with broad functionality such as HouseCall, Trend Micro's free online scanner.

Hackers, virus writers, and others who want to cause mischief or worse might use ActiveX malicious code as a vehicle to attack the system. In many cases, the Web browser can be configured so that these ActiveX controls do not execute by changing the browser's security settings to “high.”

ActiveUpdate

A Trend Micro utility that enables on-demand or background updates to the virus pattern file and scan engine, as well as the anti-spam rules database and anti-spam engine.

address

Refers to a networking address (*see* IP address) or an email address, which is the string of characters that specify the source or destination of an email message.

TERM	EXPLANATION
administrator	Refers to “system administrator”—the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.
administrator email address	The address used by the administrator of your Trend Micro product to manage notifications and alerts.
adware	Advertising-supported software in which advertising banners appear while the program is running. Adware that installs a “back door”; tracking mechanism on the user's computer without the user's knowledge is called “spyware.”
alert	A message intended to inform a system's users or administrators about a change in the operating conditions of that system or about some kind of error condition.
anti-relay	Mechanisms to prevent hosts from “piggybacking” through another host’s network.
antivirus	Computer programs designed to detect and clean computer viruses.
archive	A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.
attachment	A file attached to (sent with) an email message.
audio/video file	A file containing sounds, such as music, or video footage.

TERM **EXPLANATION**

authentication

The verification of the identity of a person or a process. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from).

The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or on public-key systems using digital signatures.

Also see public-key encryption *and* digital signature.

binary

A number representation consisting of zeros and ones used by practically all computers because of its ease of implementation using digital electronics and Boolean algebra.

block

To prevent entry into your network.

bridge

A device that forwards traffic between network segments based on data link layer information. These segments have a common network layer address.

browser

A program which allows a person to read hypertext, such as Internet Explorer. The browser gives some means of viewing the contents of nodes (or "pages") and of navigating from one node to another. A browser acts as a client to a remote Web server.

cache

A small fast memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc.

TERM	EXPLANATION
case-matching	Scanning for text that matches both words and case. For example, if “dog” is added to the content-filter, with case-matching enabled, messages containing “Dog” pass through the filter; messages containing “dog” do not.
cause	The reason a protective action, such as URL-blocking or file-blocking, was triggered—this information appears in log files.
child	The non-parent machine in a cluster, the child machine is the passive machine for active/passive scenario. Child members receive synchronized configurations from parent device.
clean	To remove virus code from a file or message.
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.
client-server environment	A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to some protocol, asking for information or action, and the server responds.
cluster	A group of machines form a cluster; and the machines in the cluster will share almost the same policies and configurations. Administrators can use the Web UI on the parent member via floating (or cluster) IP address to manage centralized policies and configurations.
cluster-level settings	IWSVA policies and settings which can be centrally managed in cluster.

TERM	EXPLANATION
cluster IP address	An IWSVA cluster has a floating IP address; administrators can always use the floating IP address to manage the cluster from Web UI and CLI. The floating (or cluster) IP address remains associated with the cluster and always points to the parent member of the cluster, even when switchover or failover occurs.
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
configuration	Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
content filtering	Scanning email messages for content (words or phrases) prohibited by your organization’s Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
content violation	An event that has triggered the content filtering policy.
cookie	A mechanism for storing information about an Internet user, such as name, preferences, and interests, which is stored in your Web browser for later use. The next time you access a Web site for which your browser has a cookie, your browser sends the cookie to the Web server, which the Web server can then use to present you with customized Web pages. For example, you might enter a Web site that welcomes you by name.
daemon	A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.

TERM	EXPLANATION
damage routine	The destructive portion of virus code, also called the payload.
default	A value that pre-populates a field in the Web console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.
De-Militarized Zone (DMZ)	From the military term for an area between two opponents where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. They might be external or internal. External DMZ Ethernets link regional networks with routers.
Deployment Wizard	A Web console-based wizard, which is used for ease of deployment. Deployment-related configurations have been removed from the product installation to this wizard.
dialer	A type of Trojan that when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge.
digital signature	Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption. *Also see* public-key encryption *and* authentication.
directory	A node, which is part of the structure in a hierarchical computer file system. A directory typically contains other nodes, folders, or files. For example, *C:\Windows* is the Windows directory on the C drive.
directory path	The subsequent layers within a directory where a file can be found, for example, the directory path for the ISVW for SMB Quarantine directory is: *C:\Programs\Trend Micro\ISVW\Quarantine*

TERM	EXPLANATION
disclaimer	A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message, To see an example, click the online help for the **SMTP Configuration - Disclaimer** screen.
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
(administrative) domain	A group of computers sharing a common database and security policy.
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called “name resolution”, uses the Domain Name System (DNS).
DoS (Denial of Service) attack	Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.

TERM	EXPLANATION
DOS virus	Also referred to as "COM" and "EXE file infectors." DOS viruses infect DOS executable programs- files that have the extensions *.COM or *.EXE. Unless they have overwritten or inadvertently destroyed part of the original program's code, most DOS viruses try to replicate and spread by infecting other host programs.
download (noun)	Data that has been downloaded, for example, from a Web site through HTTP.
download (verb)	To transfer data or code from one computer to another. Downloading often refers to transfer from a larger "host" system (especially a server or mainframe) to a smaller "client" system.
dropper	Droppers are programs that serve as delivery mechanisms to carry and drop viruses, Trojans, or worms into a system.
ELF	Executable and Linkable Format—An executable file format for UNIX and Linux platforms.
encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone might use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone might send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.

TERM	EXPLANATION
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking “I accept” during installation. Clicking “I do not accept” will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and adware into their computers when they click “I accept” on EULA prompts displayed during the installation of certain free software.
Ethernet	A local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of cable schemes, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network. The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable.
executable file	A binary file containing a program in machine language which is ready to be executed (run).
EXE file infector	An executable program with a .exe file extension. *Also see* DOS virus.
exploit	An exploit is code that takes advantage of a software vulnerability or security hole. Exploits are able to propagate into and run intricate routines on vulnerable computers.
failover	When a parent member of an cluster crashes or fails to handle traffic, IWSVA automatically performs a switchover in the cluster and elects a new machine to fill the role of the parent member of the cluster.

TERM	EXPLANATION
false positive	An email message that was "caught" by the spam filter and identified as spam, but is actually not spam.
FAQ	Frequently Asked Questions—A list of questions and answers about a specific topic.
file	An element of data, such as an email message or HTTP download.
file-infecting virus	File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. A minority of these viruses are very destructive and attempt to format the hard drive at a pre-determined time or perform some other malicious action. In many cases, a file-infecting virus can be successfully removed from the infected file. However, if the virus has overwritten part of the program's code, the original file will be unrecoverable
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
file name extension	The portion of a file name (such as .dll or .xml) which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.

TERM	EXPLANATION
filtering, dynamic	IP service that can be used within VPN tunnels. Filters are one way GateLock controls traffic from one network to another. When TCP/IP sends data packets to the firewall, the filtering function in the firewall looks at the header information in the packets and directs them accordingly. The filters operate on criteria such as IP source or destination address range, TCP ports, UDP, Internet Control Message Protocol (ICMP), or TCP responses. *Also see* tunneling and Virtual Private Network (VPN).
firewall	A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.
floating IP address	See cluster IP address.
FTP	A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.
gateway	An interface between an information source and a Web server.
grayware	A category of software that might be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it might violate your privacy. Examples of grayware include spyware, adware, and remote access tools.
group file type	Types of files that have a common theme, for example: - Audio/Video - Compressed - Executable - Images - Java - Microsoft Office

Term	Explanation
GUI	Graphical User Interface—The use of pictures rather than just words to represent the input and output of a program. This contrasts with a command line interface where communication is by exchange of strings of text.
HA	See High Availability
hacking tool	Tools such as hardware and software that enables penetration testing of a computer system or network for the purpose of finding security vulnerabilities that can be exploited.
hard disk (or hard drive)	One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks.
header (networking definition)	Part of a data packet that contains transparent information about the file or the transmission.
heuristic rule-based scanning	Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.
High Availability	High availability uses a second unit or node to ensure that the services are available even if the first unit breaks down.
HTTP	Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
host	A computer connected to a network.

TERM	EXPLANATION
hub	This hardware is used to network computers together (usually over an Ethernet connection). It serves as a common wiring point so that information can flow through one central location to any other computer on the network thus enabling centralized management. A hub is a hardware device that repeats signals at the physical Ethernet layer. A hub retains the behavior of a standard bus type network (such as Thinnet), but produces a star topology with the hub at the center of the star. This configuration enables centralized management.
ICSA	ICSA Labs is an independent division of TruSecure Corporation. For over a decade, ICSA has been the security industry's central authority for research, intelligence, and certification testing of products. ICSA Labs sets standards for information security products and certifies over 90 percent of the installed base of antivirus, firewall, IPSec, cryptography, and PC firewall products in the world today.
image file	A file containing data representing a two-dimensional scene, in other words, a picture. Images are taken from the real world, for example, through a digital camera, or they might be generated by computer using graphics software.
incoming	Email messages or other data routed *into* your network.
installation script	The installation screens used to install UNIX versions of Trend Micro products.
instance-level settings	IWSVA policies and settings which only apply to individual instances.
integrity checking	*See* checksumming.

TERM	EXPLANATION
IntelliScan	IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true-file type recognition, and scanning only file types known to potentially harbor malicious code. True-file type recognition helps identify malicious code that can be disguised by a harmless extension name.
Internet	A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.
Internet Protocol (IP)	An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.
interrupt	An asynchronous event that suspends normal processing and temporarily diverts the flow of control through an "interrupt handler" routine.
"in the wild"	Describes known viruses that are actively circulating. *Also see* "in the zoo."
"in the zoo"	Describes known viruses that are currently controlled by antivirus products. *Also see* "in the wild."
intranet	Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.
IP	Internet Protocol—*See* IP address.

TERM — EXPLANATION

IP address — Internet address for a device on a network, typically expressed using dot notation such as 123.123.123.123.

IP gateway — Also called a router, a gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.

IT — Information technology, to include hardware, software, networking, telecommunications, and user support.

Java applets — Java applets are small, portable Java programs embedded in HTML pages that can run automatically when the pages are viewed. Java applets allow Web developers to create interactive, dynamic Web pages with broader functionality.

Authors of malicious code have used Java applets as a vehicle for attack. Most Web browsers, however, can be configured so that these applets do not execute - sometimes by simply changing browser security settings to “high.”

Java file — Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet’s code is transferred to your system and is executed by the browser’s Java Virtual Machine.)

Java malicious code — Virus code written or embedded in Java. *Also see* Java file.

TERM	EXPLANATION
JavaScript virus	JavaScript is a simple programming language developed by Netscape that allows Web developers to add dynamic content to HTML pages displayed in a browser using scripts. Javascript shares some features of Sun Microsystems Java programming language, but was developed independently. A JavaScript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user’s desktop through the user’s browser. *Also see* VBscript virus.
joke program	An executable program that is annoying or causes users undue alarm. Unlike viruses, joke programs do not self-propagate and should simply be removed from your system.
KB	Kilobyte—1024 bytes of memory.
keylogger	Keyloggers are programs that catch and store all keyboard activity. There are legitimate keylogging programs that are used by corporations to monitor employees and by parents to monitor their children. However, criminals also use keystroke logs to sort for valuable information such as logon credentials and credit card numbers.
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building.
LDAP (Lightweight Directory Access Protocol)	An internet protocol that email programs use to locate contact information from a server. For example, suppose you want to locate all persons in Boston who have an email address containing the name “Bob.” An LDAP search would enable you to view the email addresses that meet this criteria.

TERM	EXPLANATION
license	Authorization by law to use a Trend Micro product.
license certificate	A document that proves you are an authorized user of a Trend Micro product.
link (also called hyperlink)	A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.
listening port	A port utilized for client connection requests for data exchange.
load balancing	Load balancing is the mapping (or re-mapping) of work to processors, with the intent of improving the efficiency of a concurrent computation.
local area network (LAN)	Any network technology that interconnects resources within an office environment, usually at high speeds, such as Ethernet. A local area network is a short-distance network used to link a group of computers together within a building. 10BaseT Ethernet is the most commonly used form of LAN. A hardware device called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 500 meters and provide low-cost, high-bandwidth networking capabilities within a small geographical area.
log storage directory	Directory on your server that stores log files.
logic bomb	Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met.

TERM	EXPLANATION
macro	A command used to automate certain functions within an application.
MacroTrap	A Trend Micro utility that performs a rule-based examination of all macro code that is saved in association with a document. macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).
macro virus	Macro viruses are often encoded as an application macro and included in a document. Unlike other virus types, macro viruses aren't specific to an operating system and can spread through email attachments, Web downloads, file transfers, and cooperative applications.
malware (malicious software)	Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.
Web console	The user interface for your Trend Micro product.
mass mailer (also known as a Worm)	A malicious program that has high damage potential, because it causes large amounts of network traffic.
Mbps	Millions of bits per second—a measure of bandwidth in data communications.
MB	Megabyte—1024 kilobytes of data.

TERM	EXPLANATION
Media Access Control (MAC) address	An address that uniquely identifies the network interface card, such as an Ethernet adapter. For Ethernet, the MAC address is a 6 octet address assigned by IEEE. On a LAN or other network, the MAC address is a computer's unique hardware number. (On an Ethernet LAN, it's the same as the Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN. The MAC address is used by the Media Access Control sublayer of the Data-Link Control (DLC) layer of telecommunication protocols. There is a different MAC sublayer for each physical device type.
Microsoft Office file	Files created with Microsoft Office tools such as Excel or Microsoft Word.
mixed threat attack	Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.
MTA (Mail Transfer Agent)	The program responsible for delivering email messages. *Also see* SMTP server.
Network Address Translation (NAT)	A standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. This allows Trusted networks with privately assigned IP addresses to have access to the Internet. This also means that you don’t have to get a registered IP address for every machine in your network.
network virus	A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure.

TERM	EXPLANATION
notification (*Also see* action and target)	A message that is forwarded to one or more of the following: - system administrator - sender of a message - recipient of a message, file download, or file transfer The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download.
offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
online help	Documentation that is bundled with the GUI.
open source	Programming code that is available to the general public for use or modification free of charge and without license restrictions.
operating system	The software which handles tasks such as the interface to peripheral hardware, scheduling tasks, and allocating storage. In this documentation, the term also refers to the software that presents a window system and graphical user interface.
outgoing	Email messages or other data *leaving* your network, routed out to the Internet.
parameter	A variable, such as a range of values (a number from 1 to 10).
parent	The central point of the cluster, a parent is the active machine for active/passive scenario. Administrators perform central management on the parent member, and cluster-level configurations are synchronized to the child member.

Term	Explanation
partition	A logical portion of a disk. (*Also see* sector, which is a physical portion of a disk.)
passive FTP	Configuration of FTP protocol that allows clients within your local area network to initiate the file transfer, using random upper port numbers (1024 and above).
password cracker	An application program that is used to recover a lost or forgotten password. These applications can also be used by an intruder to gain unauthorized access to a computer or network resources.
pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
payload	Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.
policies	Policies provide the initial protection mechanism for the firewall, allowing you to determine what traffic passes across it based on IP session details. They protect the Trusted network from outsider attacks, such as the scanning of Trusted servers. Policies create an environment in which you set up security policies to monitor traffic attempting to cross your firewall.

TERM	EXPLANATION
port	A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it.
protected network	A network protected by IWSVA (Trend Micro™ InterScan™ Web Security Virtual Appliance).
proxy	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
public-key encryption	An encryption scheme where each person gets a pair of “keys,” called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his or her private key. *Also see* authentication *and* digital signature.
purge	To delete all, as in getting rid of old entries in the logs.
quarantine	To place infected data such as email messages, infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your server.
queue	A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.

TERM	EXPLANATION
recipient	The person or entity to whom an email message is addressed.
registration	The process of identifying yourself as a Trend Micro customer, using a product Registration Key, on the Trend Micro Online Registration screen. *https://olr.trendmicro.com/registration*
Registration Key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNW8 *Also see* Activation Code
relay	To convey by means of passing through various other points.
remote access tool (RAT)	Hardware and software that allow a legitimate system administrator to manage a network remotely. However, these same tools can also be used by intruders to attempt a breach of your system security.
removable drive	A removable hardware component or peripheral device of a computer, such as a zip drive.
replicate	To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.
router	This hardware device routes data from a local area network (LAN) to a phone line's long distance line. Routers also act as traffic cops, allowing only authorized machines to transmit data into the local network so that private information can remain secure. In addition to supporting these dial-in and leased connections, routers also handle errors, keep network usage statistics, and handle security issues.
scan	To examine items in a file in sequence to find those that meet a particular criteria.

TERM	EXPLANATION
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
script	A set of programming commands that, after invoked, can be executed together. Other terms used synonymously with “script” are “macro” or “batch file.”
sector	A physical portion of a disk. (*Also see* partition, which is a logical portion of a disk.)
seat	A license for one person to use a Trend Micro product.
Secure Socket Layer (SSL)	Secure Socket Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server might run continuously (as a daemon), waiting for requests to arrive, or it might be invoked by some higher-level daemon which controls a number of specific servers.
shared drive	A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses.
signature	*See* virus signature.

TERM	EXPLANATION
signature-based spam detection	A method of determining whether an email message is spam by comparing the message contents to entries in a spam database. An exact match must be found for the message to be identified as spam. Signature-based spam detection has a nearly zero false positive rate, but does not detect “new” spam that isn’t an exact match for text in the spam signature file. *Also see* rule-based spam detection. *Also see* false positive.
single device	A machine that is not deployed in any Cluster
SMTP	Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages.
SMTP server	A server that relays email messages to their destinations.
SNMP	Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
SNMP trap	A trap is a programming mechanism that handles errors or other problems in a computer program. An SNMP trap handles errors related to network device monitoring. *See* SNMP.
spam	Unsolicited email messages meant to promote a product or service.
spyware	Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used.

TERM	EXPLANATION
subnet mask	In larger networks, the subnet mask lets you define subnetworks. For example, if you have a class B network, a subnet mask of 255.255.255.0 specifies that the first two portions of the decimal dot format are the network number, while the third portion is a subnet number. The fourth portion is the host number. If you do not want to have a subnet on a class B network, you would use a subnet mask of 255.255.0.0. A network can be subnetted into one or more physical networks which form a subset of the main network. The subnet mask is the part of the IP address which is used to represent a subnetwork within a network. Using subnet masks allows you to use network address space which is normally unavailable and ensures that network traffic does not get sent to the whole network unless intended. Subnet masks are a complex feature, so great care should be taken when using them. *Also see* IP address.
switchover	Switchover means IWSVA changes the parent role in the cluster. It can be triggered by user manually, or when system detects a failure.
target (*Also see* action and notification)	The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.
TCP	Transmission Control Protocol—TCP is a networking protocol, most commonly use in combination with IP (Internet Protocol), to govern connection of computer systems to the Internet.
Telnet	The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.

TERM	EXPLANATION
top-level domain	The last and most significant component of an Internet fully qualified domain name, the part after the last ".". For example, host *wombat.doc.ic.ac.uk* is in top-level domain "uk" (for United Kingdom).
Total Solution CD/DVD	A CD or DVD containing the latest product versions and all the patches that have been applied during the previous quarter. The Total Solution CD or DVD is available to all Trend Micro Premium Support customers.
traffic	Data flowing between the Internet and your network, both incoming and outgoing.
Transmission Control Protocol/Internet Protocol (TCP/IP)	A communications protocol which allows computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet.
trigger	An event that causes an action to take place. For example, your Trend Micro product detects a virus in an email message. This might *trigger* the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.
Trojan Horse	A malicious program that is disguised as something benign. A Trojan is an executable program that does not replicate, but instead, resides on a system to perform malicious acts, such as opening a port for an intruder.
true-file type	Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).

TERM **EXPLANATION**

trusted domain

A domain from which your Trend Micro product will always accept messages, without considering whether the message is spam. For example, a company called Dominion, Inc. has a subsidiary called Dominion-Japan, Inc. Messages from dominion-japan.com are always accepted into the dominion.com network, without checking for spam, because the messages are from a known and trusted source.

trusted host

A server that is allowed to relay mail through your network because they are trusted to act appropriately and not, for example, relay spam through your network.

tunneling

A method of sending data that enables one network to send data through another network's connections. Tunnelling is used to get data between administrative domains which use a protocol that is not supported by the internet connecting those domains.

With VPN tunneling, a mobile professional dials into a local Internet Service Provider's Point of Presence (POP) instead of dialing directly into their corporate network. This means that no matter where mobile professionals are located, they can dial a local Internet Service Provider that supports VPN tunneling technology and gain access to their corporate network, incurring only the cost of a local telephone call.

When remote users dial into their corporate network using an Internet Service Provider that supports VPN tunneling, the remote user as well as the organization knows that it is a secure connection. All remote dial-in users are authenticated by an authenticating server at the Internet Service Provider's site and then again by another authenticating server on the corporate network. This means that only authorized remote users can access their corporate network, and can access only the hosts that they are authorized to use.

TERM — **EXPLANATION**

tunnel interface

A tunnel interface is the opening, or doorway, through which traffic to or from a VPN tunnel passes. A tunnel interface can be numbered (that is, assigned an IP address) or unnumbered. A numbered tunnel interface can be in either a tunnel zone or security zone. An unnumbered tunnel interface can only be in a security zone that contains at least one security zone interface. The unnumbered tunnel interface borrows the IP address from the security zone interface. *Also see* Virtual Private Network (VPN).

tunnel zone

A tunnel zone is a logical segment that hosts one or more tunnel interfaces. A tunnel zone is associated with a security zone that acts as its carrier.

URL

Universal Resource Locator—A standard way of specifying the location of an object, typically a Web page, on the Internet, for example, *www.trendmicro.com*. The URL maps to an IP address using DNS.

VBscript virus

VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows Web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a “Click Here for More Information” button on a Web page.

A VBscript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user’s desktop through the user’s browser.

Also see JavaScript virus.

virtual IP address (VIP address)

A VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header.

TERM	EXPLANATION
Virtual Local Area Network (VLAN)	A logical (rather than physical) grouping of devices that constitute a single broadcast domain. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard.
Virtual Private Network (VPN)	A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling and encryption.
virtual router	A virtual router is the component of Screen OS that performs routing functions. By default, Trend Micro GateLock supports two virtual routers: Untrust-VR and Trust-VR.
virtual system	A virtual system is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual systems reside separately from each other in the same Trend Micro GateLock remote appliance; each one can be managed by its own virtual system administrator.

TERM	EXPLANATION
virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads might only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
virus kit	A template of source code for building and executing a virus, available from the Internet.
virus signature	A virus signature is a unique string of bits that identifies a specific virus. Virus signatures are stored in the Trend Micro virus pattern file. The Trend Micro scan engine compares code in files, such as the body of an email message, or the content of an HTTP download, to the signatures in the pattern file. If a match is found, the virus is detected, and is acted upon (for example, cleaned, deleted, or quarantined) according to your security policy.
virus trap	Software that helps you capture a sample of virus code for analysis.
virus writer	Another name for a computer hacker, someone who writes virus code.
Web	The World Wide Web, also called the Web or the Internet.
Web server	A server process running at a Web site which sends out Web pages in response to HTTP requests from remote browsers.

TERM	EXPLANATION
wildcard	A term used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a “wildcard,” can be used for any number or suit in the card deck.
working directory	The destination directory in which the main application files are stored, such as /etc/iscan/IWSVA.
workstation (also known as client)	A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.
worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.
zip file	A compressed archive (in other words, “zip file") from one or more files using an archiving program such as WinZip.
"Zip of Death"	A zip (or archive) file of a type that when decompressed, expands enormously (for example 1000 percent) or a zip file with thousands of attachments. Compressed files must be decompressed during scanning. Huge files can slow or stop your network.
zone	A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or a physical or logical entity that performs a specific function (a function zone).

Index