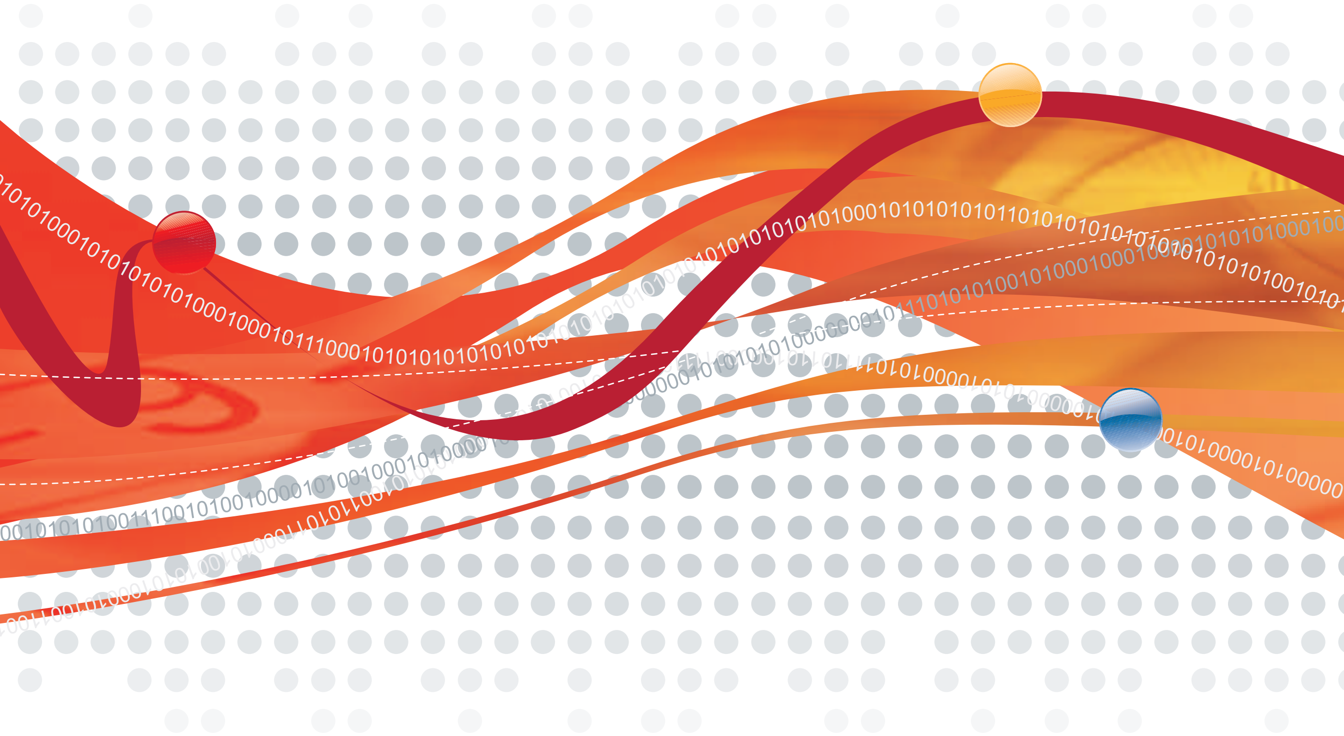
TREND MICRO™

InterScan™ Web Security Virtual Appliance 3

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 Getting Started Guide, which are available from Trend Micro's Web site at:

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

Document Part No. IBEM33647/80522

Release Date: July 2008

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 InterScan Web Security Virtual Appliance

Chapter 11: 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: Squid Configurations

Preface

Preface

Welcome to the *Trend Micro™ InterScan™ Web Security Virtual Appliance 3.1 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*

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`

Audience

The IWSVA documentation is written for IT managers and system administrators working in a medium or large enterprise environment. 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. 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
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Introducing InterScan Web Security Virtual Appliance

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

Topics in this chapter include the following:

- How IWSVA protects against HTTP and FTP security risks
- The benefits of IWSVA, its main features, and what is new in the latest version
- An explanation of the IWSVA architecture and the main program components, services, and scheduled tasks

HTTP and FTP 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, can use HTTP to spread.

Significant assessment, restoration, and lost productivity costs associated with outbreaks can be prevented. IWSVA is a comprehensive security product that protects 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.

- Web Reputation scrutinizes URLs before you access potentially dangerous Web sites, especially sites known to be phishing or pharming sites.
- URL filtering feature blocks access to Web sites with content prohibited by your organization.
- Applets and ActiveX security helps to reduce the risk of malicious mobile code by checking digital signatures at the HTTP 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 not extra cost to you.

Hardware Specifications

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

Minimum Requirements:

- Single 2.0 GHz Intel ™ Core2Duo™ 64-bit processor supporting Intel™ VT™ or equivalent
- 2GB RAM
- 8GB of disk space. IWSVA automatically partitions the detected disk space as required
- Monitor that supports 800 x 600 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 3.0 GHz Intel ™ QuadCore™ 64-bit processor or equivalent for up to 8000 users
- 4GB RAM is recommended to support up to 4000 users
- 8GB RAM is recommended to support up to 8000 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 3.1 Sizing Guide.

Compatible Directory Servers

- Microsoft Active Directory™ 2000 and 2003
- Linux OpenLDAP Directory 2.2.16
- 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 comes 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

This section describes the new features in IWSVA.

Self-contained Installation

IWSVA provides a self-contained installation which provides a purpose-build, hardened and performance tuned 64-bit operating system. This dedicated operating system installs with IWSVA to provide a turnkey solution, and a separate operating system such as Linux, Windows, or Solaris is not required.

VMware Support

IWSVA is fully supported when running on VMware ESX Server 3.5.

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.

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

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

Network Integration using Transparent Bridge Mode

IWSVA supports Transparent Bridge Mode. With Transparent Bridge Mode, IWSVA can be deployed between networking devices such as routers, switches, and firewalls without the need to reconfigure clients, servers, or network routes.

Transparent Bridge Mode provides full transparency without modification to the source and destination IP addresses or MAC addresses.

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. Host MAC and IP addresses are passed unmodified and IWSVA acts as a layer 2 bridge.

IWSVA's CLI uses industry standard syntax to provide a familiar interface for configuring the appliance.

On-box Caching by Squid 3.0

For installation convenience, IWSVA installs the open source Squid 3.0 application to provide simple on-box content caching. Squid is a widely used caching application that can help you reduce Internet bandwidth consumption and/or improve latency for cacheable content.

You can use the IWSVA CLI commands to enable or disable the Squid application to meet your needs. By default, content caching through Squid is disabled.

Support for Squid is provided through the open source community.

Threat Resources Drop-down List

The **Threat Resources** drop-down list can be found in the upper right-hand corner of the Summary page. This drop-down list allows you to quickly access Web threat protection technologies from Trend Micro's Threat Resource Center, TrendTracker, Malware/Spam Map, and Virus Encyclopedia.

Main Features

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

Support for Multiple 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. However, if multiple IWSVA devices are configured to access the same database server, policies (HTTP, URL filtering, applets and ActiveX, IntelliTunnel, access quota policies, etc.) are shared between all the servers.

The "master"/"slave" designation from the Server Farm page in the Web console only specifies how dynamic data (list of temporarily blocked URLs and list of client IP addresses suspected of spyware infection) is shared between multiple IWSVA devices.

If all the IWSVA installations share the same database, reports and logs show a consolidated view of all IWSVA devices on your network.

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 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.

IWSVA FTP scanning can be deployed onto your environment in conjunction with another FTP proxy server, or IWSVA can act as its own FTP proxy. To help ensure the security of 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 5-17.

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 or denies 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 60 categories of URLs, such as “gambling,” “games,” and “personals/dating.”

Categories are contained in the following logical groups:

- Computers/Bandwidth
- Computers/Harmful

- Computers/Communication
- Adult
- Business
- Social
- 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 7-6).

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 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 (see Enabling SNMP Trap Notifications on page 10-36).

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 optional URL Filter 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 5-6 and Web Reputation Settings on page 5-7.

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 2-7 and About IntelliTrap on page 5-15.

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 5-25.

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 5-12.

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 is also a static statistic, updated when the page is opened.
- Bandwidth
- Concurrent Connections
- CPU Usage

- Physical Memory Usage

For more information, see Real-time Statistics on page 10-2.

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 10-36.

Reverse Proxy Support

IWSVA is usually installed close to clients to protect them from security risks from the Internet. 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 clients requests, scans all content and then redirects the HTTP requests to the real Web server.

For more information, see Reverse Proxy on page 3-9.

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. There are four main classes of reports:

- Blocking event reports
- Traffic reports
- Spyware/grayware reports
- Cleanup 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 10-1.

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:** Number of accumulated detected pharming sites in a week and 28 days can be displayed in the Security Risk Report like other Web threats.
- **Reports (Real-time and Scheduled):** Blocked pharming sites show up in the following reports because the information is logged in the URL Blocking Log that is used to generate reports:
  - 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: Security Risk Report tab:** Files detected by IntelliTrap are counted as a separate risk in the report.
- **Summary Page: Scanning tab:** Files detected by IntelliTrap are listed in the “Scanning results for” with its frequency.
- Real-time Report

For more information, see Reports, Logs, and Notifications on page 10-1.

Chapter 2

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:

- An explanation of Trend Micro's ActiveUpdate feature
- How to update program components through the native IWSVA Web console or through Trend Micro Control Manager
- Configuring proxy settings to enable Internet connectivity for updates
- An explanation of the program components that need to be updated
- Getting version information about components being used by IWSVA
- Invoking manual (on-demand) and scheduled updates
- Forcing a manual update
- Verifying a successful update
- Rolling back to previous versions of pattern files or the scan engine
- Applying controlled pattern releases

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://www.trendmicro.com/download/`

Clicking the link for IWSVA takes you to the Update Center page for IWSVA. Scroll down to review the patches that are available.

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 login 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 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, IntelliTrap, and IntelliTunnel.
- Weekly
- Daily
- Hourly
- On demand (manually)

Note: Trend Micro recommends hourly updates of the pattern files and daily and weekly updates of engines.

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 both updating components from Trend Micro's update servers and for product registration and licensing.

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 = 3 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**.

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, 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 5-25.

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

- **Anti-virus scan engine:** This is the module that 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 2-3 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.

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 VSAPI 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 test after test 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 remain 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 5-6)

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/wrsonlinequer
y.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 **Scanning** 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 **Scanning** tab is active.
2. For all of the components listed on the **Scanning** tab, select components to update and then click **Update**.

   If IWSVA is already using the latest version of the component and no update is available, a message questions whether you want to force an update. Forcing an update is not necessary unless the components on the IWSVA device are corrupt or otherwise cannot be used.

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 **Summary** on the main menu.
2. Select the component to update and then click **Update**.

   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
- 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 the virus 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 virus pattern file. This forces all URL requests to be scanned, ensuring better virus 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 **Scanning** tab of the **Summary** page 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 10-35 and Enabling URL Filtering and Scan Engines Update Notifications starting on page 10-35.

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 **Summary** on the main menu.

   The **System Dashboard** tab opens by default.
2. Click the **Scanning** tab.
3. 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 **Scanning** 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're 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 and then the **Scanning** tab and confirm that the virus pattern version in use corresponds to the version of the CPR that you tried to apply.

Chapter 3

HTTP Configuration

Before you start using InterScan Web Security Virtual Appliance (IWSVA) to scan for malicious HTTP 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.

Topics in this chapter include the following:

- Enabling the HTTP Traffic Flow
- Specifying a Proxy Configuration and Related Settings
- Network Configuration and Load Handling
- Configuring an IWSVA Server Farm
- Configuring Access Control Settings
- Setting Up IWSVA ICAP

To enable and configure Squid, see Appendix E, Squid Configurations. To enable and configure WCCP, see Network Configuration and Load Handling on page 3-11 and your Cisco product documentation. To enable and configure Full Transparency (Transparent Bridge mode), see Network Configuration and Load Handling on page 3-11

Enabling the HTTP Traffic Flow

In order for your clients to access the Internet, HTTP traffic flow through IWSVA must be enabled. (HTTP traffic flow is enabled by default.) Likewise, HTTP access can be turned off from the IWSVA Web console. Trend Micro recommend you set the traffic flow before configuring the other HTTP settings discussed in this chapter.

To enable or disable the HTTP traffic flow through IWSVA:

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

   The state of HTTP traffic flowing through IWSVA appears at the top of the Scanning page.

2. Select one of the following:

   - If HTTP traffic is turned off, click the **Turn On** link to enable it.
   - If HTTP traffic is turned on, click the **Turn Off** link to disable it.

When HTTP traffic is turned off, your clients cannot access Web sites or any other services carried through HTTP. To see an example of these links at the top of the **Summary** page.

Specifying a Proxy Configuration and Related Settings

If you would like to change the deployment mode after the installation, the Installer will walk you through the deployment configuration with IWSVA. You can optionally choose the scanning mode that corresponds to the physical installation of IWSVA on the network.

- **Transparent bridge**—IWSVA passes traffic from one network device such as a switch, router, or firewall, to another device for delivery to the requesting client. IWSVA acts as a bridge between the devices and transparently scans passing HTTP and FTP traffic.

  Transparent bridge settings apply to both HTTP and FTP traffic. If you select the Transparent bridge option, FTP proxy settings are disabled. SSL (HTTPS) requests are typically fulfilled, but the content is not scanned.

If the clients and IWSVA are in the same segment, no configuration is required; otherwise, see the following 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 server** — 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.

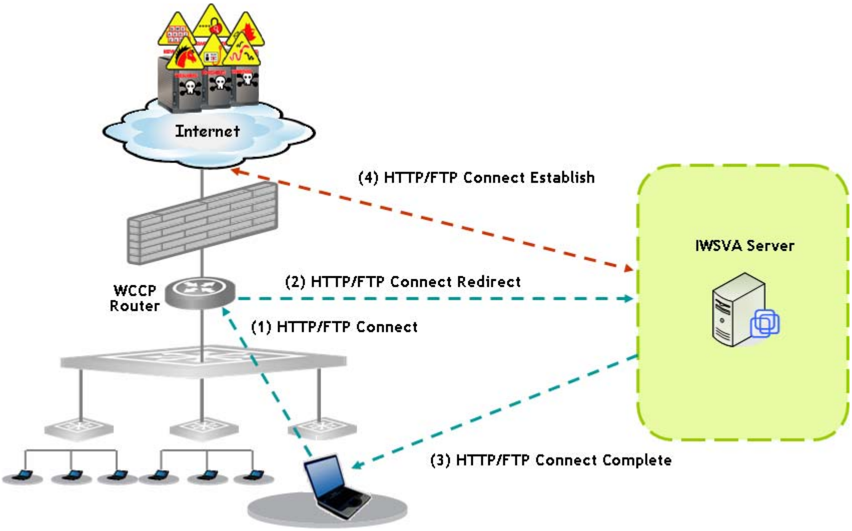

Internet
(4) HTTP/FTP Connect Establish
IWSVA Server
WCCP
Router
(2) HTTP/FTP Connect Redirect
(1) HTTP/FTP Connect
(3) HTTP/FTP Connect Complete

FIGURE 3-1 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.

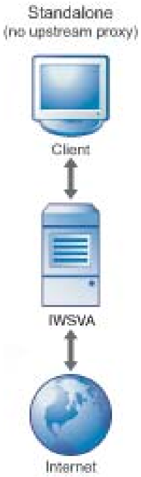


FIGURE 3-2 Forward, no upstream proxy

To configure a stand-alone installation:

1. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. Ensure that **Forward proxy** is enabled, and **Enable upstream proxy** and **Enable transparency** are not selected.
3. Click **Save**.

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: When IWSVA is configured to run in upstream proxy mode with a designated proxy server, then Trend Micro recommends that the proxy settings for Updates also be configured for a designated proxy server to allow WAN access (see Proxy Settings for Updates on page 2-3). Certain types of update events utilize the Updates proxy settings to retrieve important information.

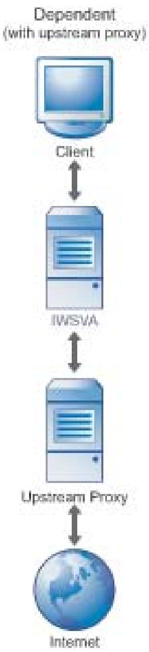


FIGURE 3-3 Forward, upstream proxy

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 Approved List will not take effect. Content from servers that you configure on the Server IP Approved List still will be scanned or filtered.

To configure IWSVA to work with an upstream proxy:

1. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. Check **Forward proxy**.
3. Check "**Enable upstream proxy**" and enter the IP address or host name of the upstream **Proxy server**, and its **Port**.
4. Click **Save**.

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 don't include information about the host.
- HTTP requests for servers that use a port other than the HTTP default port 80 are redirected to IWSVA. This means SSL (HTTPS) requests are typically fulfilled, but the content is not scanned.
- Do not use any source NAT (IP masquerade) downstream of IWSVA, because IWSVA needs to know the IP address of the client to clean.

- 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 clients' HTTP 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.

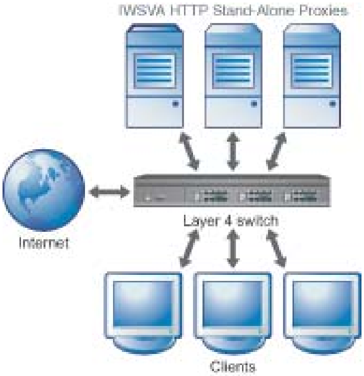


FIGURE 3-4 Forward proxy with transparency

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

To configure simple transparency:

1. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. Check **Forward proxy**.
3. Check **Enable transparency** and **Use simple transparency**.
4. Under the **Client Requests** section, change the **Listening port number** to the same port that the Layer 4 switch is configured to use.
5. Click **Save**.

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 of both directions (uploading and downloading) is scanned. Because most HTTP requests consist of an empty body, scanning files that are being uploaded is not so useful in the forward proxy configuration. In the reverse proxy configuration, there is more emphasis on scanning files that are being uploaded than in the forward proxy configuration.

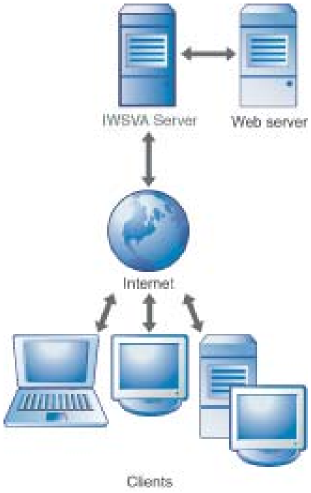


FIGURE 3-5 Reverse proxy protects Web server from clients

To configure IWSVA as a reverse proxy:

1. Select **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. Select "**Reverse proxy**", and enter the IP address or host name of the **Web server** that the reverse proxy protects.
3. Enter the **Port** (default = 80).
4. If you want to enable HTTPS access, select **Enable SSL Port** and enter the **Port Number**.
5. Click **Save**.

Note: If communication with your internal Web servers is through SSL, do not forget to configure the HTTPS ports. For more information, see HTTPS Ports starting on page 3-16.

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 set additional 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.

To configure the listening port number:

1. Open the IWSVA Web console and click **HTTP > Configuration > Proxy Scan Settings**.
2. In the “**Listening port number**” text box, type the port number (default values are 1344 for ICAP and 8080 for HTTP Proxy).
3. Click **Save**.

Note: IWSVA handles HTTPS connections differently from HTTP connections. Because the data is encrypted, IWSVA is not capable of scanning content downloaded through HTTPS. 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 **HTTP > Configuration > Proxy Scan Settings** 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 will depend on the hardware it is installed on, 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 8000 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. To support a larger or more active user community, you need to configure additional IWSVA servers to work together in a server farm (see Configuring an IWSVA Server Farm on page 3-12).

Note: For more information on capacity sizing, refer to the IWSVA 3.1 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 IWSA:
    - 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.

After setting up the IWSVA server, open the IWSVA Web console and click **HTTP > Configuration > Proxy Scan Settings** to set the corresponding IWSVA scan mode.

Configuring an IWSVA Server Farm

Multiple IWSVA devices can be used to balance traffic and scanning loads. In a multiple server configuration, one server is designated as the "master" and the other servers in the farm are designated as "slaves." Slave servers get their configuration settings from the master, and report security and program event information back to the master so administrators can view consolidated reports from all IWSVA devices on their network.

Note: An IWSVA server farm must have only one master server.

To configure server designation:

1. Open the IWSVA Web console and click **Administration > IWSVA Configuration > IWSVA Server Farm**.
2. Select **Enable for use in a multiple IWSVA server configuration**.
3. Type a value for the **Master's listening port number** (default is 1444).
4. Under **Server role**, click one of the following two options:
    - Master server
    - Slave server

      For a Slave server role, type the **Master's IP address** in the field provided.
5. Click **Save**.

Configuring Access Control Settings

IWSVA includes several configurations to control your clients' HTTP 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.

Identifying Clients and Servers

For controlling client HTTP 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 > Access Control Settings** 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 **Access Control Settings** screen.

2. Ensure that the **Client IP** tab is active.
3. Check **Enable HTTP Access Based On Client IP**.
4. Select the radio button 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 3-13.

To delete a client IP or IP range, click the corresponding **Delete** icon next to it.

5. 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.

6. Click **Save**.

Server IP Approved 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 Approved 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 approved 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 approved 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 approved list for ICAP installations.

To add servers to the Server IP Approved List:

1. Select **HTTP >Configuration > Access Control Settings** from the main menu.
2. Ensure that **Approved Server IP 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 3-13.
4. 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.
5. Access control settings are evaluated according to the order they appear in the list at the bottom of the **Approved Server IP List** tab.
6. 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 > Access Control Settings** 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. 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're allowing or denying access, click the **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 **Destination Port** tab.

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

HTTPS Ports

IWSVA can restrict which ports can be used to tunnel 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 > Access Control Settings** 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. 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.
6. 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.
7. Click **Save**.

Setting Up IWSVA ICAP

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

1. Set up an ICAP 1.0-compliant cache server.
2. Flush existing cached content from the cache appliance.

Note: The ICAP setup procedures below apply to the ICAP versions listed under X-Authenticated ICAP Headers Support on page 1-3. 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.

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.

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.

12. For multiple IWSVA ICAP server services, type the additional entries in steps 10 and 11. For example:

    For response mode,

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

    For request mode,

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

13. Click **Commit Changes**.
14. Click the **Access Control Lists** tab, then select **Enable Access Control Lists**.
15. Type "`icap (Service Farm name of the ICAP Server) any`" in **HTTP ACL**.
16. Click **Commit Changes**.
17. 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:

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.

1. Select **Management**.

   Type the logon user name and password if prompted.
2. Click **ICAP** in the left menu, then click the **ICAP Services** tab.
3. Click **New**. The **Add ICAP Service** screen opens.
4. In the **ICAP service name** field, type an alphanumeric name. Click **Ok**.
5. Highlight the new ICAP service name and click **Edit**. The **Edit ICAP Service name** screen opens.
6. Type or select the following information:
   1. The ICAP version number (that is, 1.0)
   2. 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.
   3. The maximum number of connections (ranges from 1-65535). The default value is 5.
   4. 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.
   5. Choose the type of method supported (response or request modes).
   6. Use the default preview size (bytes) of zero (0).
   7. Click **Sense settings** to retrieve settings from the ICAP server (recommended).
   8. To register the ICAP service for health checks, click **Register** under the **Health Check Options** section.
7. 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**.

8. 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**.

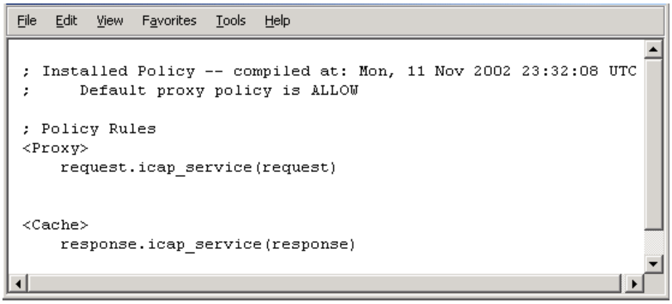
   Type the logon user name and password if prompted.
2. Click **Policy** on the left menu, then click the **Visual Policy Manager** tab.
3. Click **Start**. If the **Java Plug-in Security Warning** screen appears, click **Grant this session**.
4. On the menu bar, click **Edit > Add Web Content Policy**. 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 3-6 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**.

Enabling “X-Virus-ID” and “X-Infection-Found” Headers

IWSVA can return two optional headers from the ICAP server whenever a virus is found: the “X-Virus-ID” and the “X-Infection-Found” headers. Neither of these headers is 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-ica
p-subid-00.txt
```

To enable the X-Virus-ID header:

1. From the main menu, click **HTTP > Configuration > Proxy Scan Settings**.
2. For the **ICAP** option, select **Enable "X-Virus-ID" ICAP header** and/or **Enable "X-Infection-Found" ICAP header**.

Chapter 4

Policies and User Identification Method

InterScan Web Security Virtual Appliance (IWSVA) is able to apply different HTTP virus scanning, 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
- Default Global and Guest Policies
- Deploying Policies
- Configuring the User Identification Method
- Login Accounts

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 use 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.
- **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.

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. (The Guest Policy is supported only when IWSVA runs in HTTP Forward Proxy mode with LDAP enabled.)

Default Global and Guest Policies

IWSVA has default global and guest policies for the following HTTP activities: 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 **HTTP > Configuration > Proxy Scan Settings** after first enabling LDAP (**HTTP > Configuration > User Identification**).

Note: By default, there is no access quota control for clients who access IWSVA through the default listening port; thus there is no pre-configured Global Access Quota Policy.

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 via proxy authorization" 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" user identification method, see User/Group Name through Proxy Authorization starting on page 4-7.

Enabling the Guest Port

In order 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** from the main menu.
2. From the **User Identification** screen, select "**User/group name via proxy authorization"** and then enter the designated directory server (s) of choice.
3. Click **Save**.
4. Select **HTTP > Configuration > Proxy Scan Settings** 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 Now** 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 > Database** screen.

Note: When policies are being applied, either after the cache expiration interval or from clicking **Deploy Policies Now**, HTTP and FTP connections are interrupted for a short time (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 via proxy authorization (LDAP)

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** 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.

Host name identification relies on information included in HTTP headers by Internet Explorer. In order to utilize this identification option, a modification to the end user's Windows Registry must be made. 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 after on each PC in the network—it does not need to be run again unless the hostname of the PC is changed.

You will find the `register_user_agent_header.exe` file in `/usr/iwss/bin/register_user_agent_header.exe` on IWSVA.

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 after 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** 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)
```

that Internet Explorer includes 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.

After running the `register_user_agent_header.exe` utility, a new registry value is created under the

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Intern
et Settings\User Agent\Post Platform
```

key called `IWSS25:<host_name>/<MAC address>` are encrypted, where `<host_name>` and `<MAC address>` correspond to the client that ran the utility.

User/Group Name through Proxy Authorization

IWSVA can integrate with the following LDAP servers, and supports both the LDAP two and three protocols:

- Microsoft™ Active Directory 2000 and 2003
- 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 via proxy authorization**" method, clients are required to enter their network logon credential before accessing the Internet. The following table shows which LDAP authentication methods can be used with each of the supported LDAP servers:

TABLE 4-1. Authentication Methods for Supported LDAP Servers

	KERBEROS	SIMPLE AUTHENTICATION	NTLM
Microsoft Active Directory 2000 and 2003	yes	yes	yes
Linux OpenLDAP 2.3.39	yes	yes	no
Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server) 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**) to have IWSVA send the user's credential (used in the Admin account) as plain text for the initial LDAP connection only. For increased security protection, IWSVA uses the advance authentication method (Kerberos or Digest-MD5) for all subsequent user logon authentications from IWSVA to the LDAP server.	no	yes	no

LDAP Communication Flows

When clients request Internet content, they are prompted to enter their network credential. Simple authentication sends the network credential through clear text. Advanced authentication uses a Kerberos server as a central secure password store. Therefore, the benefit of using Kerberos is a higher degree of security. After the client's credential is authenticated with a Kerberos Server, a special encrypted "ticket" certified by the Kerberos server is used to access IWSVA and the Internet.

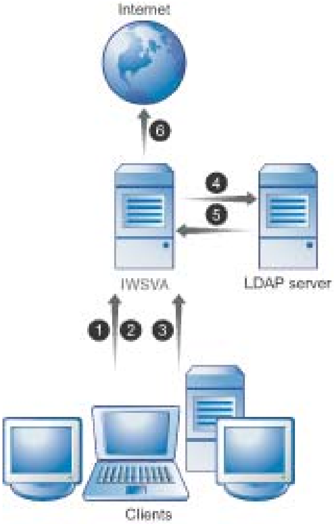


FIGURE 4-1 LDAP Communication Flow Using Kerberos Authentication

Configuring LDAP Settings

If you want to use the user/group name through proxy identification method and configure policies that are linked to your network's LDAP server, first configure your LDAP settings.

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 4-3. 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 through proxy identification method:

1. Select **HTTP > Configuration > User Identification** from the main menu.
2. Under the **User Identification Method** section, check **User/group name via proxy authorization**.
3. 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 2000 or 2003, 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, enter the **LDAP server hostname** using its FQDN (Fully Qualified Domain Name).

   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

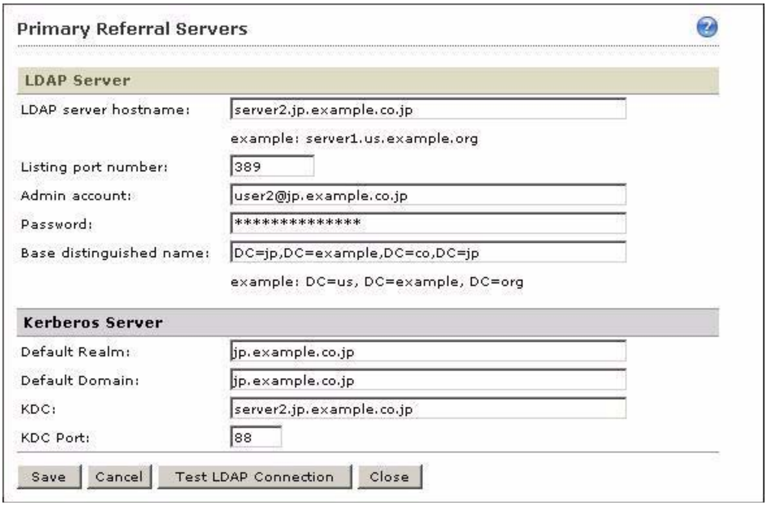
Additionally, configure the following parameters to use Advanced authentication:

- 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 in HTTP Proxy mode with Microsoft Active Directory.

11. In the event 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 **Enable Referral Chasing** and then click the **Primary referral server** and **Secondary referral server** links.
12. 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 4-2 Configure referral servers

13. 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.
14. 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 via proxy authorization” 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.

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), Trend Micro recommends creating groups with the “Universal” Group Scope to ensure that cross-domain group membership within an Active Directory forest is included in the Global Catalog.

Note: In order to configure IWSVA to listen on port 3268, the Microsoft Active Directory server that IWSVA uses should have the Global Catalog enabled.

Because 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 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 via proxy authorization user identification methods.

Note: Even if you configure IWSVA to use the Host name (modified HTTP headers) or User/group name via proxy authorization 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 4-4 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 (either **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 4-7.

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 (either **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 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 4-9.

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 (either **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 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 10-17).

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 logins 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 login CLI. This is the default access for new users.
- Auditor—Users cannot make any configuration changes; they can only view configurations, logs, and reports. They can change their own password.
- 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 > Login Accounts**.
2. In the Login Accounts page, click **Add**.
3. In the **Add Account** 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 4-17.
4. Click **Save**.

   The new login account appears in the **Login Accounts** page.

Changing a Login Account

To change a login account:

1. From the main menu, click **Administration > Login Accounts**.

2. Click on the desired username.
3. In the Edit Login Account page, 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 4-17.
4. Click **Save**.

   The changed login account appears in the **Login Accounts** page.

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 5

Configuring HTTP Scanning

This chapter describes how to configure HTTP virus scanning and applets and ActiveX security policies. Topics in this chapter include the following:

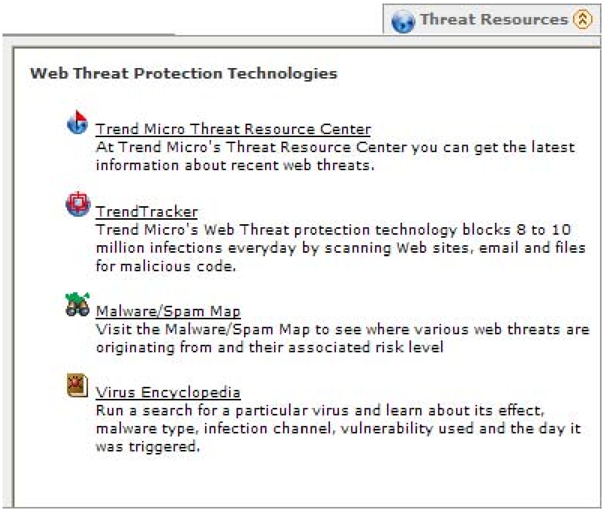
- Enabling HTTP scanning and applets and ActiveX security
- Understanding HTTP scanning settings and their effect on Web browsing performance
- Creating and modifying HTTP virus scanning, and Applet/ActiveX security policies
- Configuring HTTP virus scanning, including file type blocking, compressed file handling, large file handling, spyware and grayware scanning rules, and scan actions
- Understanding how Applet/ActiveX security works
- Configuring Java applet security, including digital signature and certificate status, applet instrumentation, and re-signing
- Configuring ActiveX security rules
- Configuring applet and ActiveX security settings

Enabling HTTP Scanning and Applets and ActiveX Security

You can enable or disable HTTP scanning from the Summary page of the 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 (see Enabling the HTTP Traffic Flow starting on page 3-2). Otherwise, clients cannot access the Internet.

From the **Threat Resources** drop-down list in the upper right-hand 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.



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 5-1 Web threat protection technologies that can be accessed in IWSVA

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 Traffic:** is shown as a red circle with a white “x”, click on the adjacent **Turn On** link to start the IWSVA HTTP proxy daemon.
3. Click **HTTP** in the left-hand column and select **Policies** under **HTTP Scan**.
4. At the top of the page, check **Enable virus scanning** and **Enable Web reputation**, then click **Save**.
5. In the left-hand column, select **Policies** under **Applets and ActiveX**.
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 extension. Trend Micro recommends that you minimize the list of MIME content-types to skip. In general, relying on the scan engine to decide whether a file should be scanned is safer than trying to pick out which file types you want to skip yourself. Firstly, the content-type HTTP header might not accurately represent the true type of the content to download. Secondly, 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: Performance might be adversely affected if the main policy for ActiveX scanning directs that all PE (windows executable) files must 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.

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.

   Web Reputation must be enabled at the global level in order for it 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 via proxy authorization*. 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 4-4 and LDAP Query Matching Across Main and Referral Servers starting on page 4-13.

   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, 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** (Account tab) screen, 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 in order for it to be used 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. Specify the URL blocking sensitivity level.

   Upon receiving the Web Reputation score, IWSVA determines whether the score is below or above 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.

4. 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 5-7.

Anti-phishing and Anti-pharming Detection

Phishing issues 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 attempts to redirect you to imposter Web sites with the intention of stealing private information (usually financial 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.

Web Reputation Settings

Web Reputation settings involve specifying the following:

- Query method
- URL exceptions
- Whether to provide feedback on infected URLs to Trend Micro
- Whether to evaluate Web Reputation in an evaluative 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:

1. Click **HTTP > HTTP Scan > Policies** from the main menu.
2. From the Scan Policies screen, click the **Enable Web Reputation** check box to either enable or disable Web Reputation.

When a Web Site is Within the Web Reputation Approved List

When a Web site is within the Web Reputation approved list, IWSS or IWSA bypasses any malicious code scans. This could cause security holes when this approved list Web site has been hacked to inject malicious code into the Web site.

IWSVA addresses this issue by turning on the malware scan feature as the default. As such, the Web page is always scanned even when Web Reputation recognizes that the Web site is within its approved list.

If your environment has performance concerns, you may consider to bypass any malicious code scans on a Web site that is within Web Reputation approved list.

To bypass any malicious code scans on a Web site that is within the Web Reputation approved list:

1. Login the terminal as `Root`.
2. Enter `su - iscan`.
3. Enter `/usr/iwss/bin/admin_wrs_scanflag.sh on`.
4. Enter `exit`.
5. Enter `/var/iwss/S99ISproxy reload+` to restart or reload iwss daemon.

To scan a Web site that is within Web Reputation approved list:

1. Login the terminal as `Root`.
2. Enter `su - iscan`.
3. Enter `/usr/iwss/bin/admin_wrs_scanflag.sh off`.
4. Enter `exit`.
5. Enter `/var/iwss/S99ISproxy reload+` to restart or reload iwss daemon.

To verify IWSVA will or will not scan a Web site within the Web Reputation approved list, you can download and test the following:

`http://us.trendmicro.com/us/support/virus-primer/eicar-test-files/eicar.com.`

If you configure IWSVA to scan a Web site within the Web Reputation approved list, the eicar file will be detected and blocked. If you configure IWSVA to bypass a Web site within Web Reputation approved list, the eicar file will be downloaded.

Specifying the Web Reputation Query Method

The default Web Reputation query method is **DNS and encrypted HTTP**. IWSVA queries the domain level (DNS) first and then the path/file level (HTTP). This is the default setting. The **Encrypted HTTP** setting encrypts all queries making it the more secure option.

To specify the Web Reputation query method:

1. Select **HTTP > Configuration > Query Method Settings** from the main menu.
2. From the Query Method Settings screen, either accept the default query method or select **Encrypted HTTP**.

Specifying Web Reputation Exceptions

Web Reputation exceptions can be defined by entering the whole Web site URL, a URL keyword, a partial URL, or by importing an existing exception list of URLs.

To specify Web Reputation exceptions:

1. Select **HTTP > HTTP Scanning > Settings | Web Reputation Approved List** tab from the main menu.
2. Either specify the match type or import the URL exception list.

   The default option is **Web site** (exact Web site).
3. Click **Save**.

   After you have specified a URL as an exception to Web Reputation, you still have the option to include it in Web Reputation by selecting the URL in the Approved List and clicking **Remove**. Click **Remove All** to include all URLs in the Approved List part of Web Reputation.

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, all, or options can be selected.

Feedback Option

In addition to the current dynamic URL Blocking List, VSAPI 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 VSAPI 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 trendmicro.com.

Negative Results

If the scan result from VSAPI 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 is sent to the backend Rating Server in a batch (each URL is sent sequentially).

Positive Results

If the scan result from VSAPI is positive, the URL in question is saved in the URL local cache. This prevents the same URL from getting scanned by VSAPI 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 off.

Clearing the 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 URL cache. Having the Web Reputation database on a remote server and building the local URL cache with this database information reduces the overhead on IWSVA and improves performance.

The following are the information types the 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 5-6)

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: Note: Clearing the cache stops and restarts the http scanning daemon. This might interrupt IWSVA service.

To clear the URL cache:

1. From the main menu, click **HTTP > Configuration > URL Cache**.
2. Click **Clear Cache**.

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, nor are they 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**, select the file types to block.
2. In the **Other file types** field, type the other file types to block, using a space to delimit multiple entries.

   See Appendix A, *Contact Information and Web-based Resources* for how to enter other files types that can be blocked, along with their corresponding MIME content-type.

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 in determining which files to scan for potential risks. Either all files are scanned (the safest approach), or only those files with certain file name extensions (considered the most vulnerable to infection) are scanned. But recent developments involving files being "disguised" by having their extensions changed has made 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 does not assume 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.

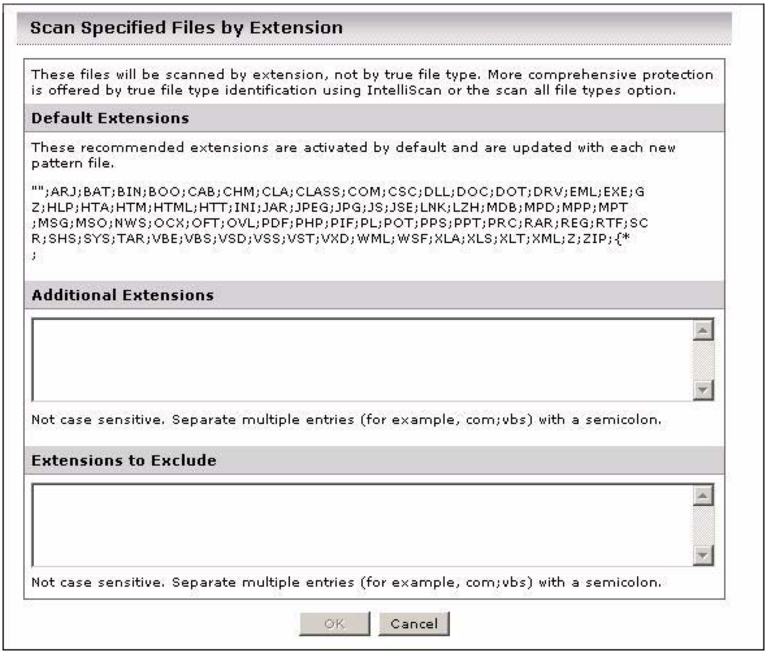
     To scan only selected file types (Trend Micro does not recommend this setting), select **Specified file extensions** and then click the list. The **Scan Specified Files by Extension** screen opens. The default extensions list shows all file types that are known to potentially harbor viruses. This list 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).

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.

```
"";ARJ;BAT;BIN;BOO;CAB;CHM;CLA;CLASS;COM;CSC;DLL;DOC;DOT;DRV;EML;EXE;G
Z;HLP;HTA;HTM;HTML;HTT;INI;JAR;JPEG;JPG;JS;JSE;LNK;LZH;MDB;MPD;MPP;MPT
;MSG;MSO;NWS;OCX;OFT;OVL;PDF;PHP;PIF;PL;POT;PPS;PPT;PRC;RAR;REG;RTF;SC
R;SHS;SYS;TAR;VBE;VBS;VSD;VSS;VST;VXD;WML;WSF;XLA;XLS;XLT;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 5-2 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 | Virus Scan Rule tab > Enable IntelliTrap** check box.

For more IntelliTrap information, see IntelliTrap Pattern and IntelliTrap Exception Pattern Files on page 2-7.

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

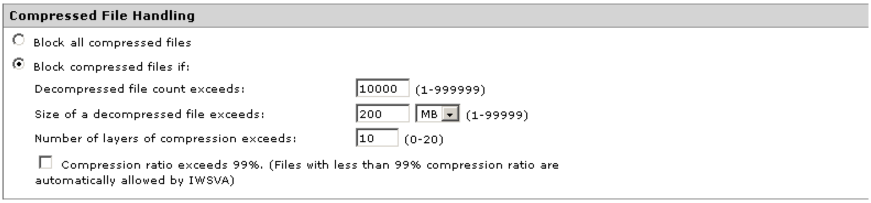
Compressed file scanning limits can be configured using the **Add** or **Edit** option for the **HTTP > Scan Policies** screen. IWSVA opens and examines the contents of compressed files according to the criteria specified in the HTTP virus scanning configuration screen. IWSVA decompresses the files according 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**, select from the following two options:

- **Block all compressed files**: All requests to download compressed files are to be fulfilled.
- **Block compressed files if...**: Requests to download compressed files that exceed the configured criteria is not fulfilled. Type values for the following parameters:
  - Decompressed file count exceeds (default is 10000)
  - 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)

A compressed file that meets any of the tests are blocked at the gateway and not scanned. For example, suppose your settings appear as follows:



Compressed File Handling

○ Block all compressed files

● Block compressed files if:

Decompressed file count exceeds: 10000 (1-999999)

Size of a decompressed file exceeds: 200 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 5-3 "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.

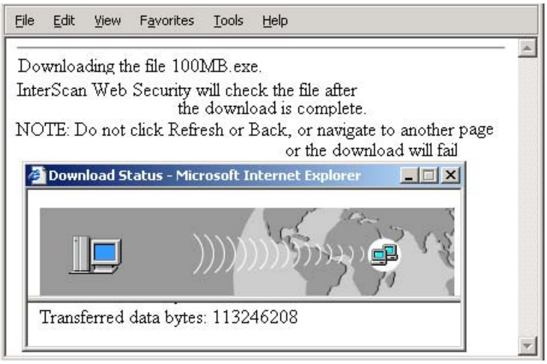
Consider configuring large file handling if your users experience browser time-outs when trying to download files. There are two large file scanning options:

Scan Before Delivering (Progress Page)

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.

In order for the progress page to work, IWSVA needs to know 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.



Downloading the file 100MB.exe.
InterScan Web Security will check the file after the download is complete.
NOTE: Do not click Refresh or Back, or navigate to another page or the download will fail

Transferred data bytes: 113246208

FIGURE 5-4 "Scan before delivering" Large File Handling Progress Window

Note: Some Internet applications (YouTube, Windows Update, streaming, etc.) will assume a certain amount of data should arrive 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.

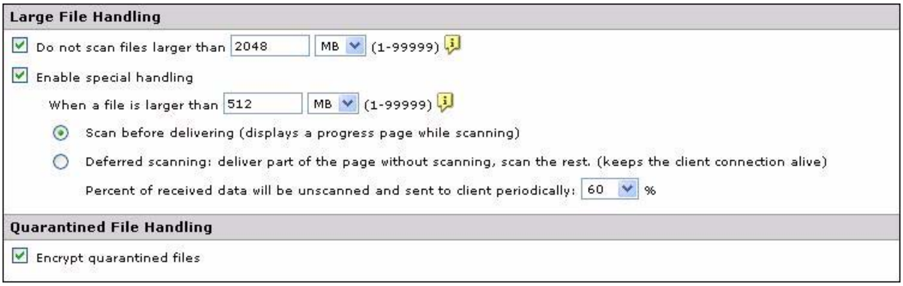
Instead of using a specified data size, IWSVA uses a percentage to define how much data is downloaded at a time. At most every two seconds, IWSVA sends a specified percentage of received data to the browser. The last chunk of data is not larger than 4KB and is sent to the browser before the scan is finished.

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 might 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 using the **Add** or **Edit** option for the **HTTP > HTTP Scan > Policies | Virus Scan Rule**.



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 5-5 For special handling of large files, there are two options to choose from: (1) scan before delivering and (2) deferred scanning

Scanning of large files can be turned off by choosing **Do not scan files larger than** to reduce performance issues when downloading very large files and you have control over their integrity.

To disable scanning large files:

- Under **Large File Handling**, check **Do not scan files larger than** and then configure the file size over which files are not scanned. The default is 2048MB.

  Disabling scanning of any files, even large ones, is not recommended, because it introduces a security vulnerability into your network.

To use large file handling for HTTP scanning:

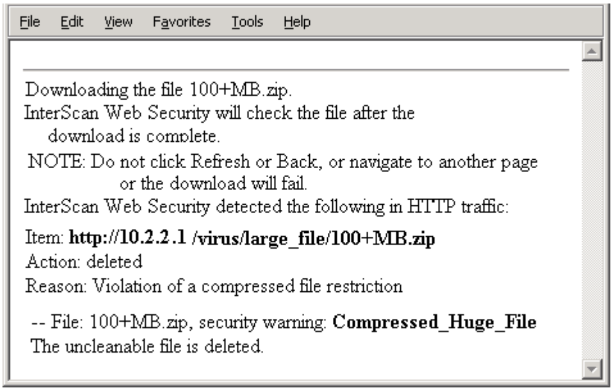
1. In the **Large File Handling** section, select **Enable special handling**, and then type the file size (in KB or MB) to be considered a large file.

   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

- 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. Users might experience time-out issues while downloading large files using FTP over HTTP.
- When using the scan-after-delivering-large-file-handling method, IWSVA does not delete files subsequently found to be infected in the first affected client.

- Violations of the large file handling policy displays a user notification in the requesting client's browser. For example:



Downloading the file 100+MB.zip.
InterScan Web Security will check the file after the download is complete.
NOTE: Do not click Refresh or Back, or navigate to another page or the download will fail.
InterScan Web Security detected the following in HTTP traffic:

Item: **http://10.2.2.1 /virus/large_file/100+MB.zip**
Action: deleted
Reason: Violation of a compressed file restriction

-- File: 100+MB.zip, security warning: **Compressed_Huge_File**
The uncleanable file is deleted.

FIGURE 5-6 Notification after Completing Scanning and Downloading the File

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 checking **Encrypt quarantined files**. This prevents the files from being inadvertently executed or opened. Note that encrypted files can only be decrypted by a Trend Micro Support engineer.

When you've completed configuring the HTTP virus scanning rules on the **HTTP > Virus Scan Add/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:

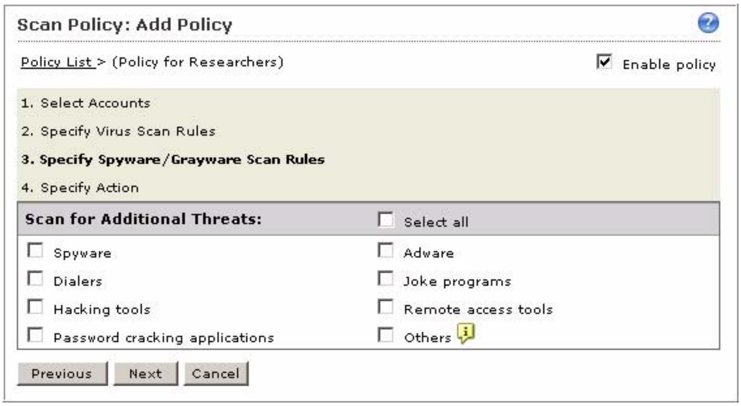
- **Spyware:** Software that secretly collects and transmits information without the user's explicit knowledge or consent
- **Dialers:** Software that secretly dials a telephone number, typically an international or pay-per call number, through the user's modem
- **Hacking tools:** Software that can 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. Under **Scan for Additional Threats** on the **HTTP > HTTP Scan > Policies > Scan Policies > |Add| Scan Policy: Add Policy (4. Specify Spyware/Grayware Scan Rules)** screen or the **Spyware/Grayware Scan Rule** tab on the **FTP > Scan Rules > FTP Scanning** screen, 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 > (Policy for Researchers) ☑ Enable policy

1. Select Accounts
2. Specify Virus Scan Rules
3. **Specify Spyware/Grayware Scan Rules**
4. Specify Action

Scan for Additional Threats: □ Select all

□ Spyware □ Adware

□ Dialers □ Joke programs

□ Hacking tools □ Remote access tools

□ Password cracking applications □ Others

FIGURE 5-7 Spyware, grayware and additional threat scan configuration

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.

  ```
  /etc/iscan/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 5-21.

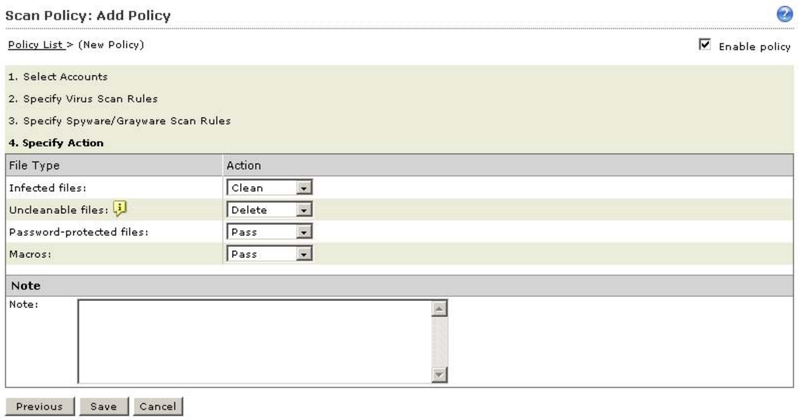
- Choose **Clean** to have IWSVA automatically clean and process infected files. The requesting client receives the cleaned file if it is cleanable, otherwise the uncleanable action is taken. This action can be applied to the *Infected files* and *Macros* scan events. For macro-containing files, the 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 in order 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 > (New Policy) ☑ Enable policy

1. Select Accounts
2. Specify Virus Scan Rules
3. Specify Spyware/Grayware Scan Rules
4. **Specify Action**

File Type	Action
Infected files:	Clean
Uncleanable files:	Delete
Password-protected files:	Pass
Macros:	Pass

Note

Note:

FIGURE 5-8 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. In order 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.

Protocols Used in Instant Messenging 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 that the site is set up 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 or 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 de-select the desired 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.

The figure below illustrates how IWSVA scans and blocks malicious applets and ActiveX objects.

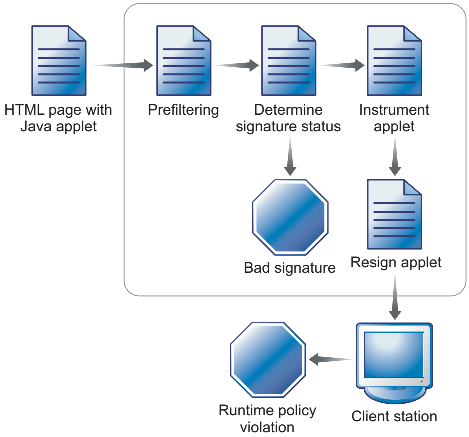


FIGURE 5-9 How Java applet security works

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.

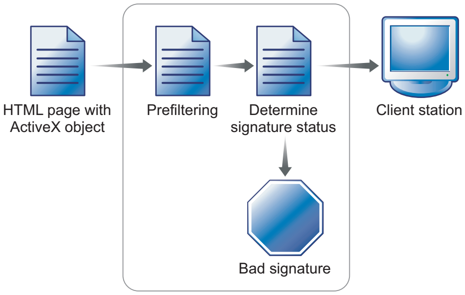


FIGURE 5-10 How ActiveX Security Works

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 for Applet Processing starting on page 5-41).

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 might 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 either the Applets and ActiveX policy page or Summary > Scanning page.

To enable malicious Applets and ActiveX scanning in HTTP traffic:

1. Select **HTTP > Applets and ActiveX > Policies** from the main menu. Alternatively, you can select **Summary** 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 4-14 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 is a verification of the integrity of the applet code against data in the signature. The second is a verification of 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 certificate known to IWSVA that is trusted. The set of these certificates can be viewed and managed by opening the Web console to **HTTP > Applets and ActiveX > 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 the **Enable** or **Disable** button to configure your security policy.
4. Click the **Exceptions** button, 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.

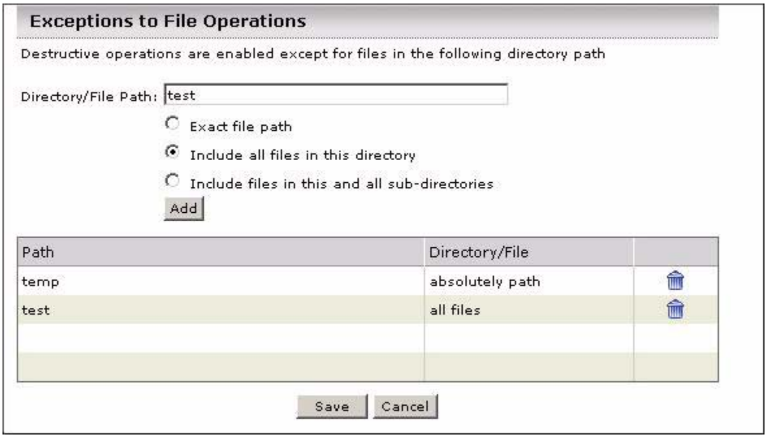
      - To configure a specific file path, check **Exact file path**.
      - To exclude the entire folder's contents from the security rule, check **Include all files in this directory**.
      - To exclude all of the folder's files, plus those in subdirectories, from the security rule, check **Include files 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 the **Add** button 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	🗑

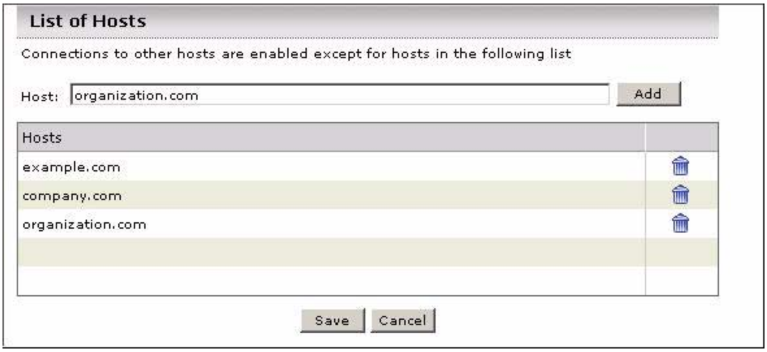
FIGURE 5-11 Java applet instrumentation settings exception files and folders

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, check **Enable** or **Disable** next to **Host connections**, then configure exceptions to the security policy.
   a. Enter the **Host** that do not apply to the configured security policy.

   b. Click the **Add** button 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:
Add
Save
Cancel

Host: organization.com

Hosts	
example.com	🗑
company.com	🗑
organization.com	🗑

FIGURE 5-12 Exceptions to the Java applet host connection rules

8. Choose **Create new thread groups** to allow applets to create new thread groups. To disallow this operation, clear it.
9. Choose **Create unlimited active threads** to have IWSVA ignore thread activity from applets downloaded to clients on the LAN. Clear the box and specify a limit to restrict the number of threads applets can create at one time.
10. Choose **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**.

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 > Applets and ActiveX > 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 > Applets and ActiveX > 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 owing to 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 countersignature.

    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**.

Managing Digital Certificates for Applet Processing

In order for IWSVA to determine that 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 root CA certificate of the signature is known to IWSVA, is active, and is not flagged.

If IWSVA encounters an unknown certificate during applet signature processing, it saves the certificate in the "inactive" list, along with the URL of the applet that contained the signature. All types of certificates are collected in this way (signing, intermediate, and root). If required later, a root 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 root 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 root 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 > Applets and ActiveX > 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 > Applets and ActiveX > 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 note that, as stated above, only active root 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 > Applets and ActiveX > 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 > Applets and ActiveX > 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 > Applets and ActiveX > 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 > Applets and ActiveX > 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.

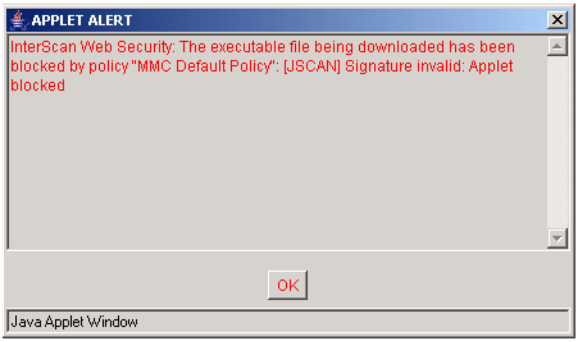
To remove a certificate from being flagged:

1. Select **HTTP > Applets and ActiveX > 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.

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:

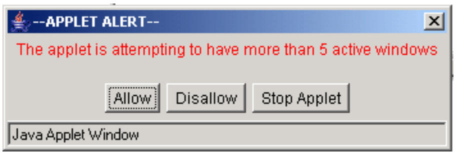


InterScan Web Security: The executable file being downloaded has been blocked by policy "MMC Default Policy": [JSCAN] Signature invalid: Applet blocked

FIGURE 5-13 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.

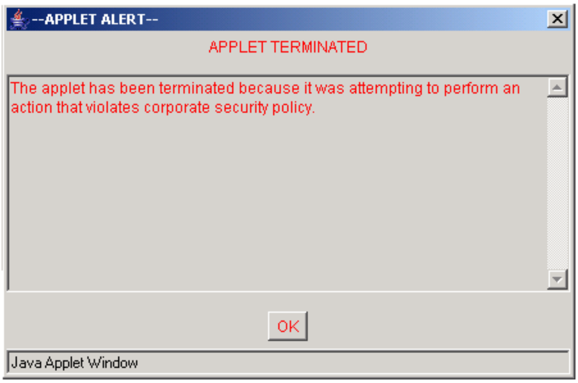


--APPLET ALERT--

The applet is attempting to have more than 5 active windows

FIGURE 5-14 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 5-15 Applet Execution Termination Notification

Chapter 6

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 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:

- Using access quota policies to set a limit on client bandwidth consumption
- Overview of URL access control
- Exempting scanning of trusted URLs to improve browsing performance to low-risk sites
- Blocking all access to sites
- Using the Phish pattern file of known phishing sites
- Submitting suspicious URLs to Trend Micro for further analysis

Introduction to Access Quota Policies

The IWSVA access quotas Guest Policy limits the HTTP bandwidth used by clients who access the Internet through the IWSVA 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 IWSVA service in a multiple server configuration environment reloads the policies according to the time-to-live (TTL) value configured on the **HTTP Configuration** page (**Administration > IWSVA Configuration > Database**).

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 via proxy authorization*. These settings are configured on the **HTTP > Configuration > User Identification** screens. 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 4-4.

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 take you 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 IWSVA 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 optional 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 optional 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, has hacking potential, or has a reputation score that deems it untrustworthy. Both the optional 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 6-4).

  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 5-6).

  If the URL is found on the Web Reputation exception list, IWSVA skips the anti-phishing and anti-pharming detection for this URL (see Specifying Web Reputation Exceptions on page 5-9).
- 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 5-7).
- The final process of Web Reputation is to determine the category of the URL (see Direct URL Filter Category Selection on page 1-7).

  The category information is used later by the optional 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 optional 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 URL Filtering module exception list, the URL bypasses the category filtering and proceeds to the final step in URL access control (see URL Filtering Exceptions on page 7-8).

  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 the Web Reputation exception list, IWSVA skips the sensitivity level checking for this URL (see Specifying Web Reputation Exceptions on page 5-9).

  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

IWSVA 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

IWSVA 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).

If you installed the HTTP stand-alone proxy handler, trusted URLs are exempted from all IWSVA modules. If you installed the ICAP proxy handler, REQMOD activities (for example, URL filtering, Webmail upload scanning, and URL blocking) cannot bypass the trusted URLs list.

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 IWSVA 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 IWSVA 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*
```

Managing your trusted URLs and exceptions:

1. Click **HTTP > URL Access Control > Trusted URLs** from the main menu.
2. In the **Trusted URLs** configuration page, select "**Enable URL trusting**."
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 > 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

IWSVA can block Web sites and URL strings in both ICAP and HTTP proxy mode.

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. The stand-alone proxy requires no additional configuration.

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 IWSVA 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 IWSVA 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, IWSVA prevents the addition and display a warning message stating that the entry already exists in the other list.

Configuring URLs to block:

1. Click **HTTP > URL Access Control > 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.)
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

IWSVA can import a list of URLs to block from a file. Write a title or comments 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 > 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 click **Import**.
4. Click **Save**.

Using a Pattern File (Phish)

Phishing is a malicious hacker term that means electronically hunting for a victim. “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 IWSVA blocks. IWSVA 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 IWSVA Web console and click **HTTP > URL Access Control > 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 IWSVA Web console and click **HTTP > URL Access Control > 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 7

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 6-4).

Topics in this chapter include the following:

- Introducing URL filtering and how URL filtering policies work
- Understanding the URL filtering workflow
- Creating, modifying and deleting URL filtering policies
- Configuring URL filtering settings, including managing URL categories, setting URL filtering exceptions to retain access to blocked sites and setting the work and leisure time schedules
- Requesting reviews of URLs misclassified into the wrong category

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.

In addition, IWSVA also 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 allows for very flexible application of the URL filtering policy. There are three basic mechanisms for customization:

- IWSVA access to the Web Reputation database that contains URLs in over 68 categories, such as "gambling," "games," and "personals/dating."

  Categories are contained in the following logical groups:

  - Computers/Bandwidth
  - Computers/Harmful
  - Computers/Communication
  - Adult
  - Business
  - Social
  - General
- Each category can be blocked or not blocked 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. In the event a

URL that your organization needs to access is associated with a prohibited category, exceptions to URL filtering can be used 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.

The following are two rules that you can apply for a given policy in a given time period:

- Block access to configured site categories during work time
- Block access to configured site categories during leisure time

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 4-4).

A URL requested by a user can be classified into one or more of 60-plus categories, which are organized into 7 groups. With the requested URL as input, the query is made to the Web Reputation database. The result of the query either allows or denies access to the requested URL.

Note: Manual updates to the URL filtering engine can be done from the **Summary** (Scanning tab) 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 not supported if you have installed IWSVA in ICAP 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 two-step process:

- Select the accounts to which the policy applies.
- Specify the Web site categories to be blocked during work and leisure time.

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 via proxy authorization (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 4-4.

5. Click **Next**.

6. On the **Specify Rules** screen, ensure that **Enable policy** is selected.

7. Select the URL categories to which you want to restrict access.

   - Select the check box of the category that you want to blocked during work time. 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. Restricted days and hours are defined on the URL Filtering Settings (Schedule tab) page.
   - Select the check box of the category that you want to block during leisure time. 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. Unspecified times are considered "leisure" times.

   The list of groups is not configurable.

8. Type an optional **Note** to include useful information about this policy for future reference.

9. Click **Save**.

10. 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.

11. Click **Save**.

12. 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 the URL categories that clients are allowed to access.
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 68 Web site categories, which are contained in 7 logical groups
- Configuring exceptions to allow access to specific Web sites that would otherwise be blocked by a URL filtering rule
- 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.

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 to suggest a reclassification.

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

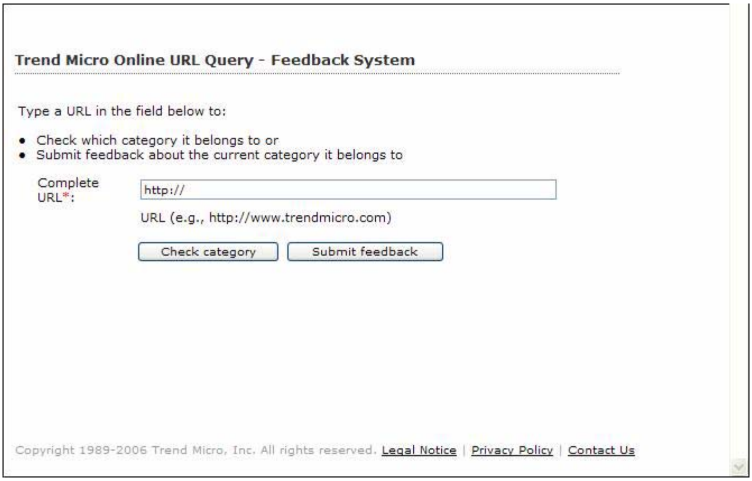
An unknown URL has a rating of zero (0) and cannot be blocked.

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)

Copyright 1989-2006 Trend Micro, Inc. All rights reserved. Legal Notice | Privacy Policy | Contact Us

FIGURE 7-1 Trend Micro Online URL Query - Feedback System screen

4. Complete all the necessary information and click **Submit Feedback**.

URL Filtering Exceptions

IWSVA provides the option to configure exceptions to URL filtering policies and exceptions to URL filtering by the Web Reputation database (see Specifying Web Reputation Exceptions on page 5-9). URL exceptions allow access to Web sites that would otherwise be blocked. If your clients have a legitimate need to view Web sites that are being blocked by URL filtering, enter the site as a URL filtering exception. In addition to entering a URL, you can also enter one of the following:

- Specific string to match within a URL

- Exact-match string to allow access to a specific file from an otherwise blocked site

The URL Filtering Exception list for URL filtering policies is maintained in the `/etc/iscan/URLFilteringExceptions.ini` file. The path for the `URLFilteringExceptions.ini` file is set using the `filtering_exception_list` parameter under the [url-filtering] section of the `/etc/iscan/IWSSPIUrlFilter.dsc` file.

To configure the URL filtering approved list:

1. Open the IWSVA Web console and click **HTTP > URL Filtering > Settings**.
2. In the **Approved URL List** tab, type the Web address, URL keyword, or exact-match string in the **Match** field. Identify this entry by selecting one of the three options:
   - Web site
   - URL keyword
   - String
3. Click **Add** to include this entry in the "**Do not filter the following sites**."

   Click **Remove** to remove highlighted entries from the list (or **Remove All** to remove all entries). To import a list of URL filtering exceptions from a file, type or click **Browse** to navigate to the location of the file in the "**Import approved list**" field, and then click **Import**.

Note: Format the URL filtering exceptions text file as follows:
line 1 = URL Filtering Import File
line 2 = [approved]
line 3 and so on:
Web sites, URL keywords, and strings, in the format `*information*`
For example:

```
URL Filtering Import File
[approved]
*www.trendmicro.com*
*www.antivirus.com*
```

To include the "*" and "?" wildcards literally, use variable %2a or %2A to represent ***** and variable %3f or %3F to represent **?**. For example, to filter the site `www.example.com/*wildcard` literally, specify the filtering rule as `www.example.com/%2awildcard` instead of `www.example.com/*wildcard`.

4. Click **Save**.

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."

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 during 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.

Chapter 8

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:

- Understanding similarities and differences between FTP and HTTP virus scanning
- Configuring FTP scanning proxy options (stand-alone vs. FTP proxy)
- Understanding data connection options (passive FTP vs. active FTP)
- Configuring FTP scanning options
- Setting FTP access control settings

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 8-3). 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.

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.

From the **Threat Resources** drop-down list in the upper right-hand 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 5-2 to view the **Threat Resources** drop-down list.

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 identify 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 5-12 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 8-7 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 all compressed files at the gateway. Alternatively, compressed files can be accepted at the gateway but blocked when you specify one of the following:

- 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 HTTP scanning as well.

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 5-18 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 5-21.

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 from the following two options:
   - Block all compressed files
   - Block 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. Switch to the **Action** tab, and select the actions for IWSVA to take in response to scanning.
13. 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 8-4).

To limit FTP access based on client IP address:

1. Click **FTP > Configuration > Access Control Settings** 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 192.168.1.x subnet. Alternatively, the Mask can be specified as a number of bits (0 to 32).
5. Click **Add** and continue entering other clients that are allowed access FTP sites.
6. Click **Save**.

Via Server IP Approved 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 > Access Control Settings** 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 3-13 for information and examples about how to identify the servers.
4. Click **Add** and continue entering other FTP sites to exempt.
5. 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 > Access Control Settings** 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 and click **Add**.
5. Continue to add other ports to allow or deny.
6. 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 9

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.

Access to the IWSVA CLI interface 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.

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.

To access the CLI interface, you will need to have the administrator account and password. IWSVA's CLI commands are separated into two categories—nonprivileged 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. Privileged commands provide full configuration control and advanced monitoring and debugging features. Privileged commands are protected by an additional layer of credentials—the Enable account and password.

TABLE 9-1. Command Line Interface Commands

COMMAND	SYNTAX	DESCRIPTION
admin db backup	admin db backup	Backup your database
admin db checkconf	admin db checkconf	Check the configuration of the database
admin db checksize	admin db checksize	Check the size of the IWSVA database
admin db reindex	admin db reindex	Reindex the IWSVA database
admin db restore	admin db restore [filename]	Restore your database from a backup
admin db truncate	admin db truncate <DATE_FIELD>	Reindex the IWSVA database
admin db vacuum	admin db vacuum	Vacuum the IWSVA database
admin shell	admin shell	Administrative shell access
admin squid vacuum	admin squid vacuum	Vacuum the squid cache
capture interface	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

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure bridge interface	configure bridge interface <internal> <external>	Configure the default bridge interface *internal* IFNAME Interface name *external* IFNAME Interface name
configure date	configure date <date> <time>	Configure date and save to CMOS *date* DATE_FIELD [DATE_FIELD] *time* TIME_FIELD [TIME_FIELD]
configure dns	configure dns <dns1> [dns2]	Configure DNS settings *dns1* IP_ADDR Primary DNS server *dns2* IP_ADDR Secondary DNS server []
configure ethernet duplex	configure ethernet duplex <ethname> <duplex>	Configure the duplex of Ethernet interface *ethname* IFNAME Interface name *duplex* DUPLEX NIC Duplex
configure hostname	configure hostname <hostname>	Configure the hostname hostname HOSTNAME Hostname or FQDN

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure ip dhcp	configure ip dhcp [vlan]	Configure the default Ethernet interface to use DHCP vlan VLAN_ID VLan ID [1-4094], default none VLan: [0]
configure ip static	configure ip static <ip> <mask> <gateway> [vlan]	Configure the default Ethernet interface to use the static IP configuration
configure ldap interval	configure ldap interval <interval>	Configure IWSVA LDAP user group membership cache interval *interval* UINT interval (in hours)
configure ldap ipuser_cache disable	configure ldap ipuser_cache disable	Disable IWSVA LDAP IP user cache
configure ldap ipuser_cache enable	configure ldap ipuser_cache enable	Enable IWSVA LDAP IP user cache
configure ldap ipuser_cache interval	configure ldap ipuser_cache interval <interval>	Configure IWSVA LDAP IP user cache interval *interval* FLOAT interval (in hours)
configure ntp	configure ntp <ntp1> [ntp2]	Configure NTP server *ntp1* ADDRESS Primary NTP server *ntp2* ADDRESS Secondary NTP server []

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure password	configure 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.
configure proxy interface	configure proxy interface <proxy>	Configure the default proxy interface *proxy* IFNAME Interface name
configure redirect ftpports	configure redirect ftpports <ports>	Configure the redirection ftp ports *ports* MULTIPORTS Redirect ports <port1;port2;...>
configure redirect httpports	configure redirect httpports <ports>	Configure the redirection http ports *ports* MULTIPORTS Redirect ports <port1;port2;...>
configure timezone Africa Cairo	configure timezone Africa Cairo	Configure timezone to Africa/Cairo location.
configure timezone Africa Harare	configure timezone Africa Harare	Configure timezone to Africa/Harare location.
configure timezone Africa Nairobi	configure timezone Africa Nairobi	Configure timezone to Africa/Nairobi location
configure timezone America Anchorage	configure timezone America Anchorage	Configure timezone to America/Anchorage location

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure timezone America Bogota	configure timezone America Bogota	Configure timezone to America/Bogota location
configure timezone America Buenos_Aires	configure timezone America Buenos_Aires	Configure timezone to America/Buenos_Aires location
configure timezone America Caracas	configure timezone America Caracas	Configure timezone to America/Caracas location
configure timezone America Chicago	configure timezone America Chicago	Configure timezone to America/Chicago location
configure timezone America Chihuahua	configure timezone America Chihuahua	Configure timezone to America/Chihuahua location
configure timezone America Denver	configure timezone America Denver	Configure timezone to America/Denver location
configure timezone America Godthab	configure timezone America Godthab	Configure timezone to America/Godthab location
configure timezone America Lima	configure timezone America Lima	Configure timezone to America/Lima location
configure timezone America Los_Angeles	configure timezone America Los_Angeles	Configure timezone to America/Los_Angeles location
configure timezone America Mexico_City	configure timezone America Mexico_City	Configure timezone to America/Mexico_City location
configure timezone America New_York	configure timezone America New_York	Configure timezone to America/New_York location

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure timezone America Noronha	configure timezone America Noronha	Configure timezone to America/Noronha
configure timezone America Phoenix	configure timezone America Phoenix	Configure timezone to America/Phoenix
configure timezone America Santiago	configure timezone America Santiago	Configure timezone to America/Santiago
configure timezone America St_Johns	configure timezone America St_Johns	Configure timezone to America/St_Johns
configure timezone America Tegucigalpa	configure timezone America Tegucigalpa	Configure timezone to America/Tegucigalpa
configure timezone Asia Almaty	configure timezone Asia Almaty	Configure timezone to Asia/Almaty location
configure timezone Asia Baghdad	configure timezone Asia Baghdad	Configure timezone to Asia/Baghdad location
configure timezone Asia Baku	configure timezone Asia Baku	Configure timezone to Asia/Baku location
configure timezone Asia Bangkok	configure timezone Asia Bangkok	Configure timezone to Asia/Bangkok location
configure timezone Asia Calcutta	configure timezone Asia Calcutta	Configure timezone to Asia/Calcutta location
configure timezone Asia Colombo	configure timezone Asia Colombo	Configure timezone to Asia/Colombo location
configure timezone Asia Dhaka	configure timezone Asia Dhaka	Configure timezone to Asia/Dhaka location
configure timezone Asia Hong_Kong	configure timezone Asia Hong_Kong	Configure timezone to Asia/Hong_Kong location

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure timezone Asia Irkutsk	configure timezone Asia Irkutsk	Configure timezone to Asia/Irkutsk location
configure timezone Asia Jerusalem	configure timezone Asia Jerusalem	Configure timezone to Asia/Jerusalem location
configure timezone Asia Kabul	configure timezone Asia Kabul	Configure timezone to Asia/Kabul location
configure timezone Asia Karachi	configure timezone Asia Karachi	Configure timezone to Asia/Karachi location
configure timezone Asia Katmandu	configure timezone Asia Katmandu	Configure timezone to Asia/Katmandu location
configure timezone Asia Krasnoyarsk	configure timezone Asia Krasnoyarsk	Configure timezone to Asia/Krasnoyarsk location
configure timezone Asia Kuala_Lumpur	configure timezone Asia Kuala_Lumpur	Configure timezone to Asia/Kuala_Lumpur location
configure timezone Asia Kuwait	configure timezone Asia Kuwait	Configure timezone to Asia/Kuwait location
configure timezone Asia Magadan	configure timezone Asia Magadan	Configure timezone to Asia/Magadan location
configure timezone Asia Manila	configure timezone Asia Manila	Configure timezone to Asia/Manila location
configure timezone Asia Muscat	configure timezone Asia Muscat	Configure timezone to Asia/Muscat location
configure timezone Asia Rangoon	configure timezone Asia Rangoon	Configure timezone to Asia/Rangoon location
configure timezone Asia Seoul	configure timezone Asia Seoul	Configure timezone to Asia/Seoul location

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure timezone Asia Shanghai	configure timezone Asia Shanghai	Configure timezone to Asia/Shanghai location
configure timezone Asia Singapore	configure timezone Asia Singapore	Configure timezone to Asia/Singapore location
configure timezone Asia Taipei	configure timezone Asia Taipei	Configure timezone to Asia/Taipei location
configure timezone Asia Tehran	configure timezone Asia Tehran	Configure timezone to Asia/Tehran location
configure timezone Asia Tokyo	configure timezone Asia Tokyo	Configure timezone to Asia/Tokyo location
configure timezone Asia Yakutsk	configure timezone Asia Yakutsk	Configure timezone to Asia/Yakutsk location
configure timezone Atlantic Azores	configure timezone Atlantic Azores	Configure timezone to Atlantic/
configure timezone Australia Adelaide	configure timezone Australia Adelaide	Configure timezone to Australia/Adelaide location
configure timezone Australia Brisbane	configure timezone Australia Brisbane	Configure timezone to Australia/Brisbane location
configure timezone Australia Darwin	configure timezone Australia Darwin	Configure timezone to Australia/Darwin location
configure timezone Australia Hobart	configure timezone Australia Hobart	Configure timezone to Australia/Hobart location
configure timezone Australia Melbourne	configure timezone Australia Melbourne	Configure timezone to Australia/Melbourne location

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure timezone Australia Perth	configure timezone Australia Perth	Configure timezone to Australia/
configure timezone Europe Amsterdam	configure timezone Europe Amsterdam	Configure timezone to Europe/Amsterdam location
configure timezone Europe Athens	configure timezone Europe Athens	Configure timezone to Europe/Athens location
configure timezone Europe Belgrade	configure timezone Europe Belgrade	Configure timezone to Europe/Belgrade location
configure timezone Europe Berlin	configure timezone Europe Berlin	Configure timezone to Europe/Berlin location
configure timezone Europe Brussels	configure timezone Europe Brussels	Configure timezone to Europe/Brussels location
configure timezone Europe Bucharest	configure timezone Europe Bucharest	Configure timezone to Europe/Bucharest location
configure timezone Europe Dublin	configure timezone Europe Dublin	Configure timezone to Europe/Dublin location
configure timezone Europe Moscow	configure timezone Europe Moscow	Configure timezone to Europe/Moscow location
configure timezone Europe Paris	configure timezone Europe Paris	Configure timezone to Europe/Paris location
configure timezone Pacific Auckland	configure timezone Pacific Auckland	Configure timezone to Pacific/Auckland location
configure timezone Pacific Fiji	configure timezone Pacific Fiji	Configure timezone to Pacific/Fiji location

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
configure timezone Pacific Guam	configure timezone Pacific Guam	Configure timezone to Pacific/Guam location
configure timezone Pacific Honolulu	configure timezone Pacific Honolulu	Configure timezone to Pacific/Honolulu location
configure timezone Pacific Kwajalein	configure timezone Pacific Kwajalein	Configure timezone to Pacific/Kwajalein location
configure timezone Pacific Midway	configure timezone Pacific Midway	Configure timezone to Pacific/Midway location
configure timezone US Alaska	configure timezone US Alaska	Configure timezone to US/Alaska location
configure timezone US Arizona	configure timezone US Arizona	Configure timezone to US/Arizona location
configure timezone US Central	configure timezone US Central	Configure timezone to US/Central location
configure timezone US East-Indiana	configure timezone US East-Indiana	Configure timezone to US/East-Indiana location
configure timezone US Eastern	configure timezone US Eastern	Configure timezone to US/Eastern location
configure timezone US Hawaii	configure timezone US Hawaii	Configure timezone to US/Hawaii location
configure timezone US Mountain	configure timezone US Mountain	Configure timezone to US/Mountain location
configure timezone US Pacific	configure timezone US Pacific	Configure timezone to US/Pacific location
disable ntp	disable ntp	Disable the time synchronization

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
disable squid	disable squid	Disable the squid proxy server
disable ssh	disable ssh	Disable the sshd daemon
disable verbose ftp	disable verbose ftp	Disable verbose FTP logs
disable verbose http	disable verbose http	Disable verbose HTTP logs
disable verbose wccp	disable verbose wccp	Disable verbose WCCP logs
enable	enable	Enable administrative commands
enable ntp	enable ntp	Enable the time synchronization
enable squid proxy downstream	enable squid proxy downstream	Enable squid proxy server before IWSVA
enable squid proxy upstream	enable squid proxy upstream	Enable squid proxy server after IWSVA
enable ssh	enable ssh	Enable the sshd daemon
enable verbose ftp	enable verbose ftp	Enable verbose FTP logs
enable verbose http	enable verbose http	Enable verbose HTTP logs
enable verbose wccp	enable verbose wccp	Enable verbose WCCP logs
exit	exit	Exit the session

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
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
monitor ftp	monitor ftp	Monitor the FTP log.
monitor http	monitor http	Monitor the HTTP log.
monitor squid	monitor squid	Monitor the squid log.
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 9-1. 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
show arp	show arp [dest]	Display system arp tables *dest* ADDRESS Remote IP address to arp []
show capture	show capture [filename]	Display packets captures *filename* STRING [filename] []
show config all	show config all	View the all the config files.
show config db	show config db	View the db config files.
show connections	show connections	Display system connections.
show conntrack	show conntrack	Display state tracked connections.
show conntrack expect	show conntrack expect	Display state tracked connections
show daemons	show daemons	Display running system daemons.

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show date	show date	Display current date/time
show disk partition	show disk partition [partition]	Report filesystem usage *partition* STRING [optional partition] []
show disk partition readable	show disk partition readable [partition]	Report readable filesystem usage *partition* STRING [optional partition] []
show disk space	show disk space [target]	Report file space usage *target* STRING [optional directory or filename] [/]
show disk space readable	show disk space readable [target]	Report readable file space usage *target* STRING [optional directory or filename] [/]
show ethernet	show ethernet <ethname>	Display Ethernet card settings *ethname* IFNAME Interface name
show file IWSSPIJavascan	show file IWSSPIJavascan	View the IWSSPIJavascan config file
show file IWSSPIProtocolFtp	show file IWSSPIProtocolFtp	View the IWSSPIProtocolFtp config file.
show file IWSSPIProtocolHttpProxy	show file IWSSPIProtocolHttpProxy	View the IWSSPIProtocolHttpProxy config file
show file IWSSPIProtocolIcap	show file IWSSPIProtocolIcap	View the IWSSPIProtocolIcap config file

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show file IWSSPIScanVsapi	show file IWSSPIScanVsapi	View the IWSSPIScanVsapi config file.
show file IWSSPISigScan	show file IWSSPISigScan	View the IWSSPISigScan config file
show file IWSSPIUrlFilter	show file IWSSPIUrlFilter	View the IWSSPIUrlFilter config file
show file intscan	show file intscan	View the intscan config file
show firewall filter	show firewall filter	Display firewall filter
show firewall nat	show firewall nat	Display firewall nat.
show hostname	show hostname	Display network hostname.
show interfaces	show interfaces	Display network interface information
show ip address	show ip address	Display network address.
show ip dns	show ip dns	Display network dns servers.
show ip gateway	show ip gateway	Display network gateway.
show ip route	show ip route	Display network routing table.
show kernel messages	show kernel messages	Display kernel messages
show kernel modules	show kernel modules	Display modules loaded in the kernel

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show kernel parameters	show kernel parameters	Display running kernel parameters
show ldap groupcache interval	show ldap groupcache interval	Display IWSVA LDAP user group membership cache interval
show ldap ipuser_cache	show 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 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show ldap ipuser_cache interval	show ldap ipuser_cache interval	Display IWSVA LDAP IP user cache interval.
show log admin	show log admin [log_suffix]	View the admin log file *log_suffix* LOGSUFFIX [log_suffix] []
show log ftp	show log ftp [log_suffix]	View the ftp log file *log_suffix* LOGSUFFIX [log_suffix] []
show log http	show log http [log_suffix]	View the http log file *log_suffix* LOGSUFFIX [log_suffix] []
show log mail	show log mail [log_suffix]	View the mail log file *log_suffix* LOGSUFFIX [log_suffix] []
show log postgres	show log postgres	View the postgres log
show log squid	show log squid	View the squid proxy log
show log tmudump	show log tmudump	View the tmudump log file
show log update	show log update [log_suffix]	View the update log file *log_suffix* LOGSUFFIX [log_suffix] []
show metrics ftp	show metrics ftp	Display IWSVA ftp performance metrics
show metrics http	show metrics http	Display IWSVA http performance metrics
show ntp	show ntp	Display the ntp server configuration

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show open files	show open files [target]	Display open files *target* STRING [optional directory or filename] []
show open sockets	show open sockets	Display open network socket statistics
show process	show process [target]	Display process information *target* STRING [optional name/ID with wildcard support] []
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>
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 redirect	show redirect	Display the redirection port numbers
show redirect ftpports	show redirect ftpports	Display the FTP redirection port numbers.
show redirect httpports	show redirect httpports	Display the HTTP redirection port numbers.

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
show statistic disk	show statistic disk	Display disk statistics.
show statistic ethernet a	show statistic ethernet a	Display both listening and non-listening sockets.
show statistic ethernet all	show statistic ethernet all	Display all network interfaces.
show statistic ethernet n	how statistic ethernet n	Display numerical host addresses.
show statistic io	show statistic io	Display Central Processing Unit (CPU) statistics and input/output statistics for devices, partitions and network file systems (NFS)
show statistic memory	show statistic memory	Display memory statistics
show timezone	show timezone	Display network timezone
show version	show version	Display IWSVA version
show webserver port	show webserver port	Display Web server port settings.
shutdown	shutdown [time]	Shutdown this machine after a specified delay or immediately *time* UINT Time in minutes to shutdown this machine [0]
stop process	stop process <pid>	Stop a running process *pid* UINT <pid>

TABLE 9-1. Command Line Interface Commands (Continued)

COMMAND	SYNTAX	DESCRIPTION
stop process core	stop process core <pid>	Stop a running process and generate a core file *pid* UINT <pid>
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 []
wget	wget <url> <path>	Download file through HTTP/FTP protocols. *url* STRING [http://user-name:password@host-name/path] *path* FILENAME The local path to download file

Chapter 10

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:

- Understanding the Summary screen with system dashboard and reports
- Introducing blocking event, traffic, spyware/grayware and cleanup reports
- Configuring report settings and setting the report's scope
- Generating real-time and scheduled reports
- Customizing reports, and several examples of sample IWSVA report content
- Configuring the various IWSVA logs
- Querying and viewing logs
- Configuring log settings
- Exporting log data to CSV files and querying logs using Microsoft Excel
- Introducing notifications, including configuring email notification settings
- Using tokens in notifications to dynamically provide event information
- Using SNMP notifications

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 gives access to the following information:

- Real-time Statistics
- Scanning Activity
- URL Activity
- Spyware Activity
- Security Risk Reporting

Real-time Statistics

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

- Virus and Spyware Trend Display
- Hard Drive Display
- Bandwidth Display
- Concurrent Connections Display
- CPU Usage Display
- Physical Memory Usage Display

“Virus and Spyware Trend” is a static statistic that is generated when you open the **Summary** (System Dashboard tab) page. “Virus and Spyware Trend” is not updated over time like the other real-time statistics.

Virus and Spyware Trend Display

This is a static display that shows the rate at which viruses and spyware are coming up against your system. (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 installation (single server and up to a server farm).

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. See Email Notification Settings on page 10-27 and Enabling SNMP Trap Notifications on page 10-36.

Bandwidth Display

This is a dynamic display that shows the bandwidth usage of both inbound and outbound traffic for HTTP and FTP. IWSVA sees 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, which gives 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: Because each day's bandwidth usage 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.

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 10-27 and Enabling SNMP Trap Notifications on page 10-36.

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 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: Because each day's CPU usage 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.

You can specify the threshold alert value and the frequency of the alert so that you are notified when a CPU 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 10-27 and Enabling SNMP Trap Notifications on page 10-36.

Physical Memory Usage Display

This is a dynamic display that shows the amount of physical memory used by the local IWSVA computer.

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: Because each day's physical memory 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.

You can specify the threshold alert value and the frequency of the alert so that you are notified when physical memory 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 10-27 and Enabling SNMP Trap Notifications on page 10-36.

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)
- Updating and rolling back of patterns, signatures, databases, and engines

- Displaying malware names and frequency of occurrence in scanning results by selected time period
- Refreshing scanning results
- Displaying current IWSVA version

The **Scanning** tab displays the current versions, the last update date, and the update scheduled (if any) of the following components:

- Virus pattern
- PhishTrap signature database
- Spyware patterns
- IntelliTrap pattern
- IntelliTrap exception pattern
- IntelliTunnel signatures
- Virus scan engine
- URL filtering engine

URL Activity

Activities pertaining to URL activity are available from the **URL** tab. URL activity by selected time period displays the URL or category blocked and the frequency of occurrence of the following items:

- Most blocked URL
- Most blocked URL category
- Most blocked phishing site

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 where 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 gives 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 access— such as URL filtering and offending URLs detected by Web Reputation

Instant Messaging — detected by IntelliTunnel

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. To allow you to share the latest program information with those who need it, IWSVA can send notifications through email when a scheduled report is ready for viewing.

Types of Reports

IWSVA can generate the following categories of reports:

- **Blocking event reports:** Reports about virus detections, policy violations, and blocked URLs
- **Traffic reports:** Reports about Web browsing activity, the most popular Web sites and downloads, and other details about Web browsing activity
- **Spyware/Grayware reports:** Reports about spyware detections
- **Cleanup reports:** Reports about DCS cleanup attempts requested by IWSVA
- **Individual/per user reports**

The following sections describe all available reports.

Blocking-event Reports

IntelliTrap is used in real-time reports to detect potentially malicious code in real-time, compressed executable files that arrive with HTTP data. When IntelliTrap detects a malicious executable file, the detection appears in Blocking-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 blocked Applets and ActiveX objects*
- Most blocked URLs
- Most blocked URLs by day of the week
- Most blocked URLs by hour
- IntelliTunnel report

* Requires a separate license.

Individual/per User Reports

- Overview report

- Most popular sites by user
- Most blocked URLs by user
- Most blocked URL categories by user*
- URL activity by user

* Requires a separate license.

Traffic Reports

For traffic reports, you need to enable “Log HTTP/FTP access events” in **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
- Daily traffic report
- Top categories (weighted)*
- Activity level by day of the week
- Activity level by hour

* To access the top categories report, you must have a URL Filtering activation code.

Spyware/Grayware Reports

- Spyware/grayware cleanup by category
- Top spyware/grayware detections
- Top user with Spyware/Grayware infections

Cleanup Reports

- Cleanup events by category*
- Top cleanup events by name*

- Most infected IP addresses*

* Requires a separate license.

Report Settings

When generating a real-time report or setting up scheduled reports, you need to specify the information in this section.

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 name, or LDAP directory entry
- **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**. For more information about user identification, see Configuring the User Identification Method starting on page 4-4.

Report Type (Consolidated or Individual)

In Scheduled Reports, IWSVA can generate consolidated reports, that contain all possible reports. In either Scheduled Reports or Real-time Reports, IWSVA can generate individual reports that you specify. For a list of available reports, see Types of Reports starting on page 10-8.

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 report notification email message when the report is 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.

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**).
3. Click **Range** to generate a report in a given time range, and then select the **From** and **To** dates.
4. 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 10-13.
5. Under **Report Type**, select the desired report parameter(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 10-1. Report Parameter Availability Depends on the Report Type

REPORT BY	INCLUDED REPORT PARAMETERS
All users	Includes all listed report parameters except for "Individual user reports"
Specific users	Includes only the "Individual user reports" parameters
All groups or Specific groups	The following reports are enabled: - Most violations by group* - Most blocked URL categories* - Most blocked Applets and ActiveX objects - Most blocked 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**).

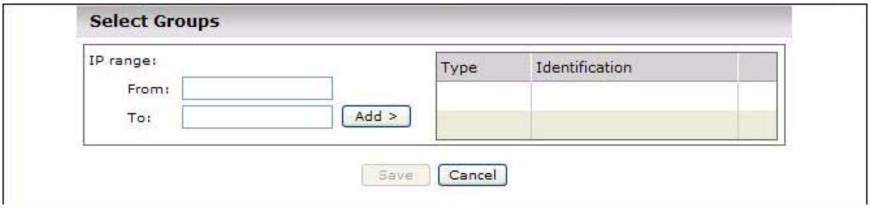


FIGURE 10-1 **Configuring a Report's Scope using the User/group (LDAP) or IP Address Range Identification Method**

3. Type the IP address range (or search for a group name in your LDAP directory if using the "User/group name via proxy authorization" 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**).

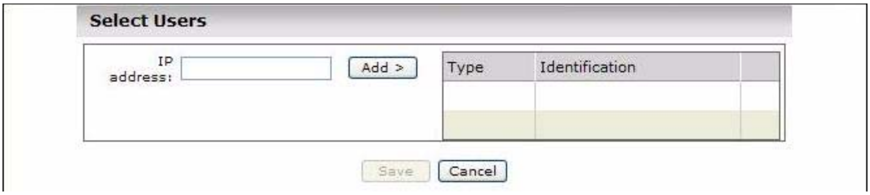


FIGURE 10-2 **Configuring a Report's Scope using the User/group (LDAP) Identification Method or IP Address Range**

3. Type the **IP address**, **Host name** or search for a user name in your LDAP directory if using the "User/group name via proxy authorization" 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 manage the large volume of reports generated, IWSVA allows you to generate only the reports that you specify and delete unnecessary scheduled reports from the archive directory.

To configure scheduled reports:

1. Click **Reports > Scheduled Reports** from the main menu.
2. Click the tab that corresponds to the frequency of scheduled report to run—either **Daily**, **Weekly** or **Monthly**.
3. Select **Enable <*Frequency*> Report**.
4. Click the **Report Settings** link.
5. Set the time and date to generate the scheduled report.
6. Under **Report by**, select the scope of the report:
   - All users
   - Specific user(s)
   - All groups
   - Specific group(s)

Note: For more information about configuring specific users or groups, see To select specific group(s): starting on page 10-12 and To select specific user(s): starting on page 10-13.

7. Under **Report Type**, select the type of report to be generated:
   - Consolidated report
   - **Individual report** If you opt for the individual reports, select the type(s) of reports to include.
8. Under **Options**, select the chart type from the menu—either **Bar**, **Stacked bar**, or **Line**.

To denote blocked traffic from unblocked traffic using different shading, select "**Distinguish blocked from unblocked traffic.**"

9. Under **Recipients**, in the "**Send report notification to**" field, type the email address(es) where IWSVA should send a notification when a newly generated report is ready for viewing. Separate multiple email addresses with a comma.
10. Click **Save**.

To delete scheduled reports:

1. Click **Reports > Scheduled Reports** in the main menu.
2. Click the tab that corresponds to the reports to delete—either **Daily**, **Weekly**, or **Monthly**.
3. Select the reports to remove and then click **Delete**.

Customizing Reports

IWSVA allows you to customize 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 ten.

You can configure IWSVA to archive scheduled reports. The default path for archiving reports is `/etc/iscan/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 **Customize the Number of Records**, type the number of records to include in each of the reports.
3. Under **Report Archives**, type the following information in the fields provided:
   a. **Archive Directory** to save the reports (the default is `/etc/iscan/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)

4. 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
- Performance
- 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:

- HTTP scan
- FTP scan
- Mail delivery daemon
- Administration, Update, and Audit trails

The database stores all log data. Log data can also be stored in text log files for compatibility with previous IWSVA versions and to permit additional data analysis using customer script. 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.

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 > Settings** (see Log Settings starting on page 10-23 for more information). Text logs provide backward compatibility with previous versions of IWSVA and allow further analysis of log data through custom scripts or other third-party applications. You can also use them to validate the completeness and accuracy of the data logged to the database.

There is a performance penalty for enabling the access log (**Log HTTP/FTP access events** is disabled by default). If you do not enable the access log, many reports on user activities are 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 **Logs > Settings > Reporting Logs > Options**.

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 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 > 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.

Virus Log

The virus log contains information about viruses that IWSVA has detected.

To view the virus log:

1. Click **Logs > 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 the **Sort by** section, select an option by which to sort the display log.
5. Click **Show Log**.

   The **Virus Log** screen opens.
6. 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, and user ID of the client involved.

To view the spyware/grayware log:

1. Click **Logs > 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 the **Sort by** section, select a sort option (Grayware, Date, Action, Category, Scan Type, File Name, User ID).
5. Click **Show Log**. The **Spyware/Grayware 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 blocking 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 > URL Blocking 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 **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 **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 access quota, file type, URL memory block list, content filter, or Phish

5. Click **Show Log**. The **URL Blocking Log** viewing screen opens.
6. 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 Access Log

The URL access log contains URL access information. IWSVA writes to the URL access log only when **Log HTTP/FTP access events** is enabled (**Log HTTP/FTP access events** is disabled by default) under **Logs > 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 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 > URL Access 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 option.
4. Click **Show Log**. The **URL Access Log** viewing screen opens.
5. Click **Refresh** to update the URL access log.

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 > 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.

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 > 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 > 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.

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 > 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 viruses 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, and Subtype).
5. Click **Show Log**. The **Cleanup Log** viewing screen opens.
6. 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 > Settings** screen.

To delete one or more logs:

1. Click **Logs > Deletion** in the main menu.
2. On each of the four tabs (**Virus Log**, **URL Blocking Log**, **URL Access Log** and **Performance 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)
- Number of days to keep the system logs

- Whether to gather performance data or log HTTP/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 > Deletion** screen. Database logs cannot be manually deleted—a deletion schedule can be configured on the **Logs > Settings** screen.

Log File Folder Locations

You can configure the folders for the reporting logs and the system logs. The default location is `/etc/iscan/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.

To configure reporting log directories:

1. Click **Logs > 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 > 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 = 5 days).

Reporting Logs

On the **Reporting Logs** tab, you can configure IWSVA to gather performance data and log HTTP/FTP access events. If you enable these, configure the logging interval.

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.2008.07.04
```

which can be read as virus log for July 4, 2008

The naming conventions for each type of log are described in the table below:

TABLE 10-2. Log Files Naming Conventions

VIRUS LOG	virus.log.yyyy.mm.dd
URL BLOCKING	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

TABLE 10-2. Log Files Naming Conventions (Continued)

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

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 10-3. 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 device.

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.

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:

- **Administrator notifications** provide information about HTTP scanning, HTTP file blocking, FTP blocked file type, FTP scanning, threshold alerts, restricted tunnel traffic, 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 HTTP scanning, HTTP file blocking, FTP scanning, URL blocking, FTP blocked file type, 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 running the setup program, but email settings can also be modified post-installation in the Web console's **Email Settings** screen.

To configure email settings for administrator notifications:

1. Click **Notifications** on the main menu.
2. On 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 initial 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 10-4. Description of Variables

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
HTTP and FTP Scanning		

TABLE 10-4. Description of Variables (Continued)

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
%Y	Date and time	The date and time of the triggering event
%F	File name	The name of the file in which a risk is detected, for example, anti_virus_test_file.htm
%V	Malware name (virus, Trojan, etc.)	The name of the risk detected
%A	Action taken	The action taken by IWSVA
%M	Moved to location	The quarantine folder location where a file was moved
%H	IWSVA host name	The IWSVA host name where the event was triggered
%N	User name	
%R	Transfer direction	
%U	URL/URI	
%X	Reasons/block type	
HTTP/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 10-4. 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	Sends its own mail	
%X	Reason	
%Y	Date and time	
%Z	Policy name	
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 Blocking		
%H	IWSVA host name (only works in header field)	
%U	URL/URI (only works in body)	
%X	Reason (only works in body)	

TABLE 10-4. Description of Variables (Continued)

VARIABLE	VARIABLE MEANING	HOW THE VARIABLE IS USED
URL Filtering		
%U	URL/URI	
%X	Reason	
Threshold Notification		
%m	Metric	
%t	Threshold value	

Configuring Notifications

To configure a notification, select the types of events that issues the notification and 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 separately uploaded to a Web server, and Trend Micro recommends using absolute links to help avoid broken links.

Configure HTTP 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 Scanning.

To configure HTTP scanning notifications:

1. Click **Notifications** and then click **HTTP 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 10-28.
4. Type the **Headline** to appear in the browser.

   The default is *IWSVA Security Event (Server Name)*. The header line is common for virus infection messages, file-type blocking, and URL blocking messages.
5. 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.

   c. Verify that the notifications appear correctly by clicking **Preview**.
6. Click **Save**.

Configuring HTTP 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 file blocking notifications:

1. Click **Notifications** and then click **HTTP 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 10-28.
4. For **Headline**, type the header line to appear in the browser.

   The default headline is *IWSVA Security Event (%h)*. The headline is common for virus infection messages, file-type blocking, and URL blocking messages.
5. For the **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.

6. Verify the notifications by clicking **Preview**.
7. Click **Save**.

Configuring a User Notification Message for Blocked URLs

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 blocked URLs:

1. Click **Notifications** in the main menu, then click **URL Blocking**.
2. Under **User Notification Message for Restricted or Blocked URLs**:
   a. Click **Default** to display the default warning message.
   b. 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.
3. Verify the notifications by clicking **Preview**.
4. 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 10-28.
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.

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 5-25.

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 10-28
4. Click **Save**.

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 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 10-28.
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.

5. Click **Save**.

Enabling Pattern File Update Notifications

IWSVA can send notifications when the product attempts to update engines or pattern files

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 triggers a notification. You can configure notifications for **Successful**, **Unsuccessful** or **Not needed** update attempts.
   b. Type a **Subject** for the notification message
3. Click **Save**.

Enabling URL Filtering and Scan Engines Update Notifications

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 scan 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 scan engine and/or 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 scan engine and/or URL filtering engine, type the **Subject** of the notification email message.
4. Click **Save**.

Enabling Threshold Alerts Notifications

You can specify threshold alert values and the frequency of alerts so that you are notified when any of the following reach 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 10-27 and Enabling SNMP Trap Notifications on page 10-36.

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 10-28.
4. Click **Save**.

Enabling SNMP Trap Notifications

IWSVA supports sending SNMP traps in response to security, update, or program events.

In order to send SNMP traps, you first need to configure the SNMP settings and then enable this feature. To do this, choose **Administration > IWSVA Configuration > SNMP Settings**.

To enable sending SNMP traps:

1. Click **Notifications** on the main menu and then click **SNMP Notification Settings**.

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)
3. Click **Save**.

Chapter 11

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. There are six types of tests to perform:

- Upload scanning
- FTP scanning
- URL blocking
- Download scanning
- URL filtering
- Applets and ActiveX scanning

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 anti-virus 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
```

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**) and local browser before testing. If either cache contains a copy of the test virus, it's 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 your Web Reputation, 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

Trend Micro recommends that you test virus scanning of Web-based mail attachments.

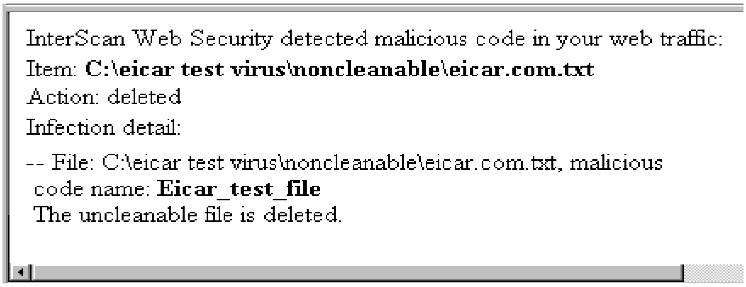
To test virus scanning of Web-based mail attachments:

1. Open the IWSVA console and click **HTTP > Scan Policies** in the main menu. Clear **Enable virus scanning**, and then click **Save**.
2. Download the test virus 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 > Scan Policies** in the main menu, select **Enable virus scanning**, and then click **Save**.

5. Send a message with one of the test viruses as an attachment by using any Internet mail daemon. A message similar to the following should appear in your browser.



InterScan Web Security detected malicious code in your web traffic:
Item: **C:\eicar test virus\noncleanable\eicar.com.txt**
Action: deleted
Infection detail:
-- File: C:\eicar test virus\noncleanable\eicar.com.txt, malicious
code name: **Eicar_test_file**
The uncleanable file is deleted.

FIGURE 11-1 This warning screen shows the detection of an EICAR test virus.

Testing FTP Scanning

The following procedure contains instructions to test your FTP virus scanning capability in stand-alone 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 (`10.2.10.2`), FTP server (`10.2.10.10`).

   Open a command line prompt and type the following:

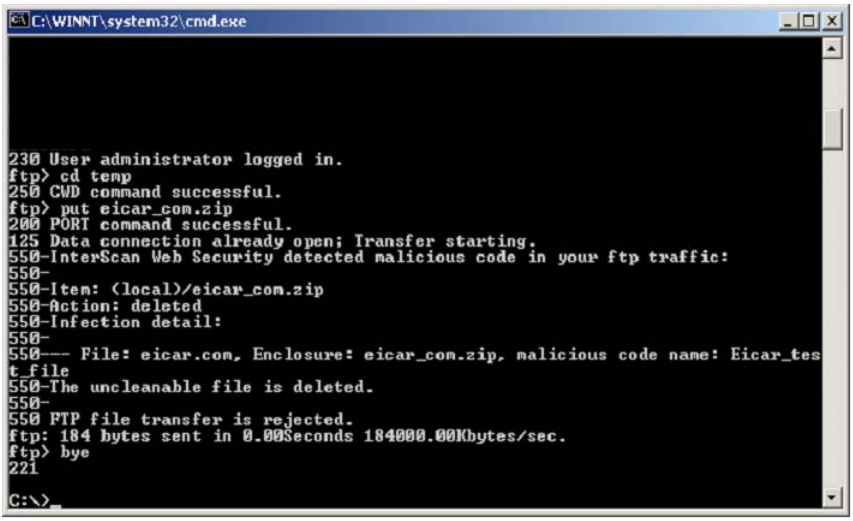
   ```
   ftp 10.2.10.2
   ```

3. Log on as `user@host.` For example, if your FTP account name is `anonymous` and the IP address of the FTP server is `10.2.10.10`, then log on as `anonymous@10.2.10.10`

4. Upload the test virus (for example, eicar_com.zip) by typing the command:

   ```
   put eicar_com.zip
   ```

5. If you have configured the IWSVA FTP proxy mode correctly, IWSVA displays a message similar to the following.



```
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 11-2 This is a warning message that shows the detection of a virus in eicar_com.zip.

Testing URL Blocking

Before attempting to test URL blocking, you must configure the correct proxy settings on the **Proxy Scan Settings** screen (click **HTTP > Configuration > Proxy Scan Settings** in the main menu).

To test URL blocking:

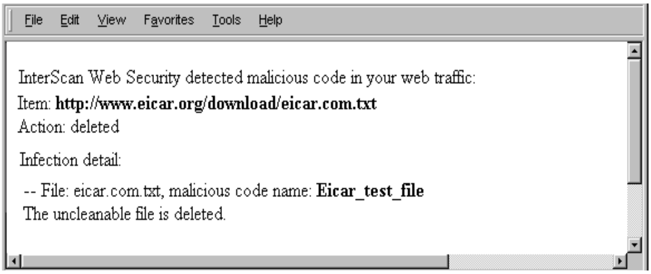
1. From the main menu, click **HTTP > URL Access Control > URL Blocking** in and then select **Enable URL blocking**.
2. Select either **Web site**, **URL keyword**, or **String** to specify the match type.
3. In the **Match** field, type either the full Web address, the URL keyword, or an exact-match string.
4. Click **Block** and then **Save**.

5. Open a Web browser and try to access the blocked Web site, a URL containing the string, or the exact-match string. A message appears in the browser.

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`



InterScan Web Security detected malicious code in your web traffic:
Item: **http://www.eicar.org/download/eicar.com.txt**
Action: deleted

Infection detail:

-- File: eicar.com.txt, malicious code name: **Eicar_test_file**
The uncleanable file is deleted.

FIGURE 11-3 The above 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.

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 categories that you want blocked during work and leisure times.
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.

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.

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 device HTTPS:

1. From the main menu, click **Administration > 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).

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 Traffic Flow on page 3-2).

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 4-4). 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 via proxy authorization** 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. Click **HTTP > Configuration > Proxy Scan Settings** from the main menu.
2. 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.
3. Click **Save**.

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 **Access Control Settings** 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 approved list to exempt frequently visited sites from scanning and filtering.

To configure which clients are allowed to access the Internet:

1. Click **HTTP > Configuration > Access Control Settings** 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. On the **Approved Server IP List** tab, configure the IP addresses of servers that are exempt from scanning, URL filtering, and URL blocking.
4. Click **Save**.

Adding or Removing a System Patch

From time to time, Trend Micro makes system patches available through the Update Center. After downloading the latest patch from the Update Center to a desktop or other computer, you can upload it to the IWSVA device where it is automatically installed.

The *patch uninstall* utility only removes the last patch installed. For example, if you have installed four patches over a one-year period, you can only remove the 4th patch—not the 3rd, 2nd or 1st.

To add a system patch:

1. From the main menu, click **Administration > System Patch** and then click the **Browse** button.
2. Locate the patch you downloaded from the Trend Micro Update Center, and then click **Upload** to have IWSVA copy the patch to the IWSVA device and begin installing.

   Only a properly formatted and encrypted Trend Micro patch can be upload from this utility.

To remove a system patch:

1. From the main menu, click **Administration > System Patch** and then click the install link for the most recently installed patch. The preview page appears, where you can confirm the version of the patch you want to remove.

   You can remove the most recently installed system patch at any time.
2. After reviewing the version and so on, 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**.
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 time to live (TTL) interval.

To configure Time to Live (TTL):

1. Open the IWSVA Web console and click **Administration > IWSVA Configuration > Database**.
2. Under **Cache Expiration (TTL in Minutes)**, type a value for the following parameters:
   - Access quota 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 GUI 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 password admin
   ```

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 > Login Accounts** in the main menu.
2. Click the user account for which you want to change the password.
3. From the Edit Login Account 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 mode by accessing the **Administration > Web Console** screen and setting the **Port number** for SSL mode to 8443, they should also specify this port number in the **HTTP > Configuration > Access Control Settings** screen (see Using SSL with Damage Cleanup Services (DCS) on page 11-13).

If this port number is not specified in the **Access Control Settings** 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 > Access Control Settings**, 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 optional URL filtering module, review the post-install tasks here to prepare IWSVA for your environment.

IWSVA accesses the Web Reputation database that contains URLs in over 60 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 > Settings** from the main menu.
2. On the **Approved URL List** tab, enter or import Web sites to 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 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 via proxy authorization 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 setting "***user_groups_central_cache_interval***" in the ***[user-identification]*** section of ***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 ***intscan.ini***. 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
- Submitting suspicious files to Trend Micro for analysis
- Web-bases resources

Contacting Technical Support

In the United States, Trend Micro representatives can be reached through phone, fax, or email. Our Web site and email addresses follow:

```
http://www.trendmicro.com
http://esupport.trendmicro.com/
support@trendmicro.com
```

General US phone and fax numbers follow:

```
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
```

IWSVA Core Files for Support

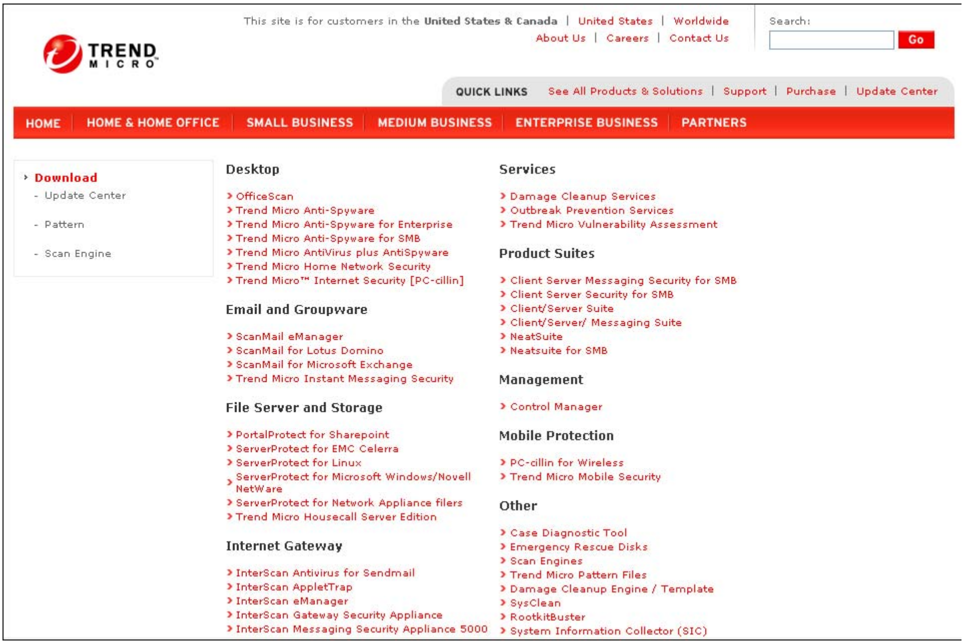
IWSVA generates a core file containing the system data held in memory when a process is abnormally terminated.

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.


This site is for customers in the United States & Canada | United States | Worldwide
About Us | Careers | Contact Us
Search:
Go
QUICK LINKS See All Products & Solutions | Support | Purchase | Update Center
HOME
HOME & HOME OFFICE
SMALL BUSINESS
MEDIUM BUSINESS
ENTERPRISE BUSINESS
PARTNERS
› Download
- Update Center
- Pattern
- Scan Engine

Desktop

- › OfficeScan
- › Trend Micro Anti-Spyware
- › Trend Micro Anti-Spyware for Enterprise
- › Trend Micro Anti-Spyware for SMB
- › Trend Micro AntiVirus plus AntiSpyware
- › Trend Micro Home Network Security
- › Trend Micro™ Internet Security [PC-cillin]

Email and Groupware

- › ScanMail eManager
- › ScanMail for Lotus Domino
- › ScanMail for Microsoft Exchange
- › Trend Micro Instant Messaging Security

File Server and Storage

- › PortalProtect for Sharepoint
- › ServerProtect for EMC Celerra
- › ServerProtect for Linux
- › ServerProtect for Microsoft Windows/Novell NetWare
- › ServerProtect for Network Appliance filers
- › Trend Micro Housecall Server Edition

Internet Gateway

- › InterScan Antivirus for Sendmail
- › InterScan AppletTrap
- › InterScan eManager
- › InterScan Gateway Security Appliance
- › InterScan Messaging Security Appliance 5000

Services

- › Damage Cleanup Services
- › Outbreak Prevention Services
- › Trend Micro Vulnerability Assessment

Product Suites

- › Client Server Messaging Security for SMB
- › Client Server Security for SMB
- › Client/Server Suite
- › Client/Server/ Messaging Suite
- › NeatSuite
- › Neatsuite for SMB

Management

- › Control Manager

Mobile Protection

- › PC-cillin for Wireless
- › Trend Micro Mobile Security

Other

- › Case Diagnostic Tool
- › Emergency Rescue Disks
- › Scan Engines
- › Trend Micro Pattern Files
- › Damage Cleanup Engine / Template
- › SysClean
- › RootkitBuster
- › System Information Collector (SIC)

FIGURE A-1 Trend Micro Technical Support site

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

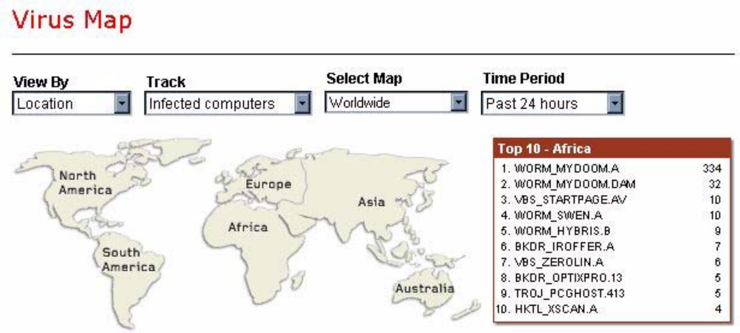
Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

`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

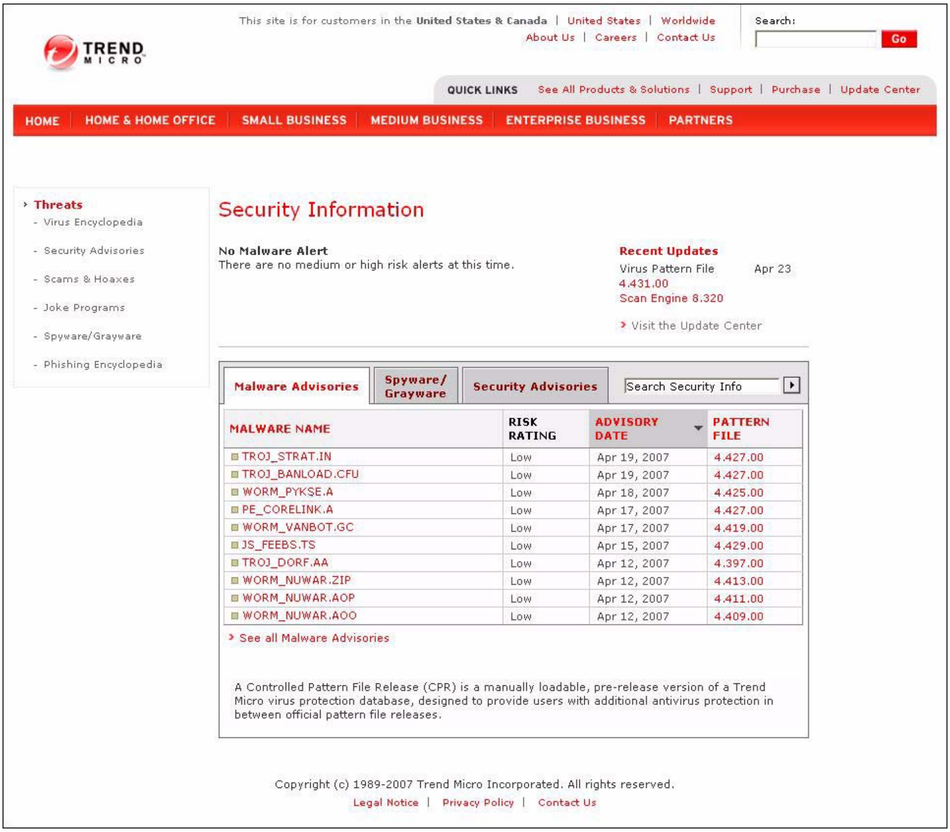
Time Period: Past 24 hours

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



TREND MICRO
This site is for customers in the United States & Canada | United States | Worldwide
About Us | Careers | Contact Us
Search:
Go
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
Malware Advisories
Spyware/ Grayware
Security Advisories
Search Security Info

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 file types that you can enter in the HTTP and FTP virus scanning policy **Other file types** fields to block corresponding MIME content-types. For example, if you type `afc`, both the `audio/aiff` and `audio/x-aiff` MIME content-types are blocked.

TABLE B-1. File Type Mapping to MIME Content-FIles

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
afc	audio/aiff	avs	video/ avs-video	bin	application/ x-binary
afc	audio/x-aiff	audiovideo	video/	binhex	application/ binhex
ani	application/ octet-stream	base64	application/ base64	binhex	application/ binhex4
arc	application/ octet-stream	bin	application/ mac-binary	binhex	application/ mac-binhex

TABLE B-1. File Type Mapping to MIME Content-FIles (Continued)

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
arj	application/octet-stream	bin	application/macbinary	binhex	application/mac-binhex40
asf	video/x-ms-asf	bin	application/octet-stream	binhex	application/x-binhex40
bin	application/x-macbinary	bmp	image/bmp	bmp	image/x-windows-bmp
bw	image/x-sgi-bw	bzip2	application/x-bzi2	cgm	image/cgm
cmx	application/x-cmx	cmx	image/x-cmx	com	application/octet-stream
core	application/octet-stream	cpio	application/x-cpio	dcr	application/x-director
doc	application/wordperfect	dwg	application/acad	dwg	application/x-acad
dwg	drawing/x-dwg	dwg	image/vnd.dwg	dwg	image/x-dwg
eps	application/postscript	eps	image/x-eps	exec	application/octet-stream

TABLE B-1. File Type Mapping to MIME Content-FIles (Continued)

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
exec	application/x-msdownload	exe	application/octet-stream	fh9	image/x-freehand
fli	video/x-fli	fm	application/vnd.framemaker	gif	image/gif
gzip	application/x-gzip	gzip	encoding/x-gzip	hpexe	application/octet-stream
iff	audio/x-aiff	java	text/x-java-source	java	application/java-class
java	application/x-java-applet	java	application/x-java-vm	java	text/x-java-source
java	application/java-class	java	application/x-java-applet	java	application/x-java-vm
jpeg	image/jpeg	jpeg	image/pjpeg	lha	application/x-lha
lisp	application/x-lisp	maud	audio/x-ma ud	midi	audio/midi
mif	application/x-mif	mng	video/x-mng	mp3	audio/mpeg
mp3	audio/mpeg3	mp3	audio/x-mpeg-3	mp3	video/mpeg
mp3	video/x-mpeg	mpeg	video/mpeg	mscab	application/x-cainet-win32-x86

TABLE B-1. File Type Mapping to MIME Content-FIles (Continued)

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
msdoc	application/ msword	msexl	application/ excel	msexl	application/ x-msexcel
msexl	application/ x-excel	msexl	application/ vnd.ms-excel	msmdb	application/ x-msaccess
msppt	application/ mspower-point	msppt	application/ powerpoint	msppt	application/ vnd.ms-powerpoint
msproj	application/ vnd.ms-project	msproj	application/ x-msproject	msproj	application/ x-project
mswri	application/ mswrite	pcx	image/ x-pcx	pdb	application/ x-pilot-pdb
pdf	application/ pdf	pdf	application/ x-pdf	pfb	application/ x-font
pict	image/ pict	pict	image/ x-pict	picture	image/
png	image/png	ppm	image/ x-portable-pixmap	ps	application/ postscript
psd	application/ octet-stream	qtm	video/ quicktime	ra	audio/ vnd.rn-realaudio
ra	audio/ x-pn-realaudio	ra	audio/ x-realaudio	rar	application/ rar

TABLE B-1. File Type Mapping to MIME Content-FIles (Continued)

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
ras	image/ x-cmu-raster	ras	image/ cmu-raster	risc	application/ octet-stream
rmf	application/ vnd.rn-real-media, g_audiovideo	rtf	application/ rtf	rtf	application/ x-rtf
rtf	text/ richtext	scm	application/ vnd.lotus-screencam	scm	application/ x-lotuss-creencam
scm	application/ x-screen-cam	scm	video/ x-scm	sf	audio/ x-sf
swf	application/ x-shock-wave-flash	tar	application/ x-tar	tga	image/ tga
tiff	image/ tiff	tnef	application/ ms-tnef	tnef	application/ vnd.mstnef
txt	text/plain	uuencode	text/ x-uuencode	zip	application/ zip
voc	audio/voc	voc	audio/ x-voc	wav	audio/wav
wbc	application/ x-webshots	wmf	application/ x-msmeta-file	wmf	image/ x-wmf

Appendix C

Architecture and Configuration Files

Topics in this appendix include the following:

- Main Components
- Main Services
- Scheduled Tasks
- About Configuration Files
- Protocol Handlers
- Scanning Modules

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 into 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 Traffic Flow on page 3-2 and Enabling FTP Traffic and FTP Scanning on page 8-4). 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 into 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 installed. 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:

- Software packages tested to enable Kerberos authentication when using IWSVA with OpenLDAP
- Modifying OpenLDAP configuration files
- Sample user and group entries in LDIF format

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

- 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/slapcat  [-v]  [-c]  [-d  level] [-b suffix] [-n dbnum]
[-f slapd.conf]
```

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.

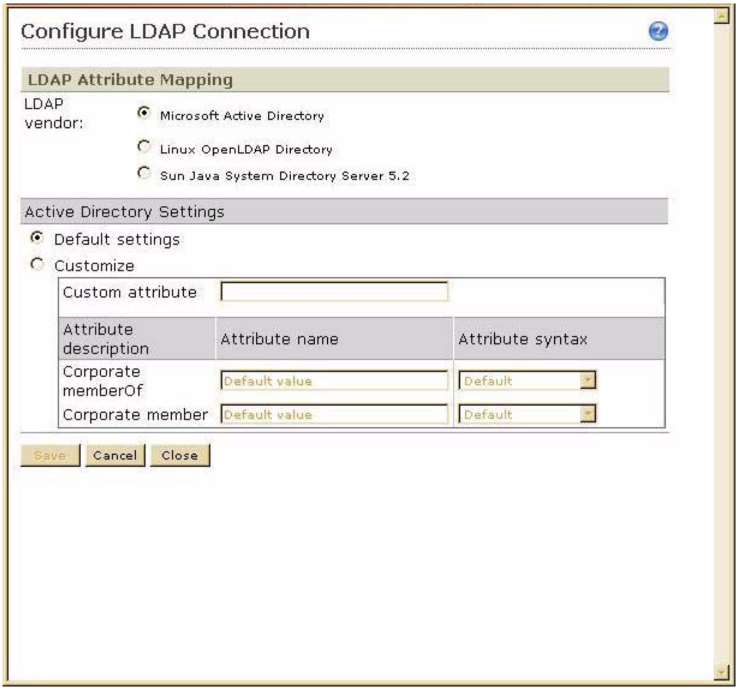
```
ldapsearch -x -D "cn=admin,dc=peter,dc=com" -w admin -b
"dc=peter,dc=com" -s sub "uid=petery" mail
```

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

Active Directory Settings

● Default settings
○ Customize

Custom attribute:

Attribute description	Attribute name	Attribute syntax
Corporate memberOf	Default value	Default
Corporate member	Default value	Default

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 three options to configure this setting, namely {"Common Name (CN)", "Distinguished Name (DN), "Customized Attribute"}.

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

The following are simplified example of a user and group entry in LDIF format:

```
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
```

FIGURE D-2 Sample user entry in LDIF format

```
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
```

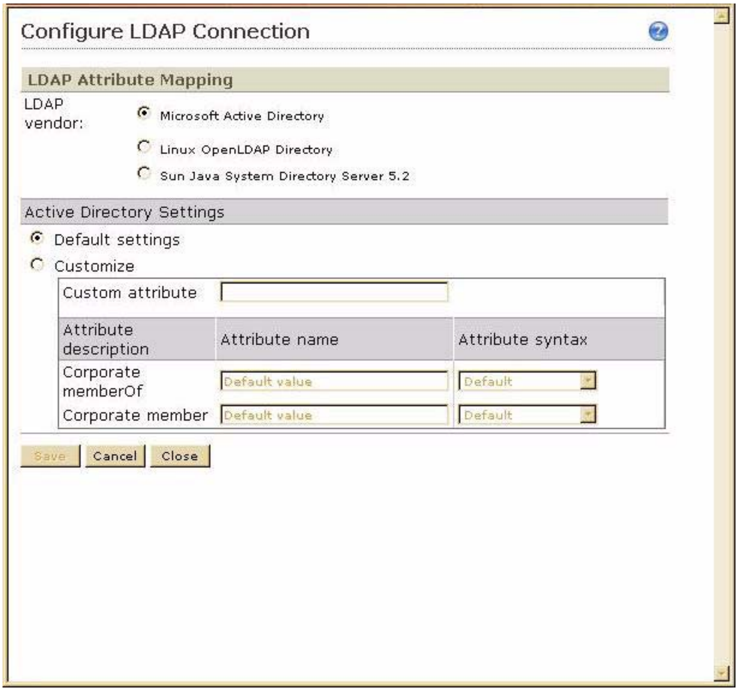
FIGURE D-3 Sample group entry in LDIF format

Note of 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

Active Directory Settings

● Default settings
○ Customize

Custom attribute:

Attribute description	Attribute name	Attribute syntax
Corporate memberOf	Default value	Default
Corporate member	Default value	Default

FIGURE D-4 OpenLDAP attribute mapping configuration screen

```
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
```

FIGURE D-5 Sample user entry in LDIF format

```
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
```

FIGURE D-6 Sample group entry in LDIF format

Take note the of 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

Squid Configurations

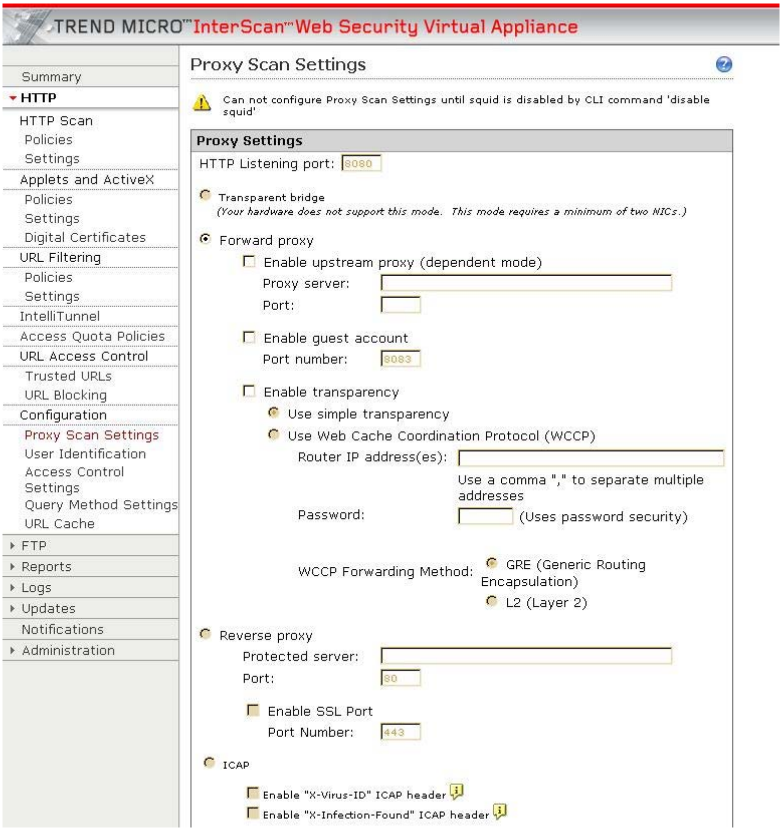
Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. It reduces bandwidth and improves response times by caching and reusing frequently-requested Web pages. IWSVA includes Squid 3.0 as a mechanism for providing on-box caching.

Squid service is disabled by default. IWSVA supports two types of Squid deployment modes:

- Squid Proxy Downstream Mode
- Squid Proxy Upstream Mode

Note: If you configure IWSVA to enable Squid service, in the **HTTP > Configuration > Proxy Scan Settings** page of the Web Console, you will see IWSVA in Forward proxy mode. You cannot switch to Transparent Bridge mode, Reverse Proxy mode, or ICAP mode using the Web console.

You will have to disable Squid service before you can configure the **HTTP > Configuration > Proxy Scan Settings** page. See the figure below. If Proxy Scan Settings is not in Forward Proxy mode, you cannot enable Squid.



Proxy Scan Settings

Can not configure Proxy Scan Settings until squid is disabled by CLI command 'disable squid'

Proxy Settings

HTTP Listening port: 8080

○ Transparent bridge
(Your hardware does not support this mode. This mode requires a minimum of two NICs.)

● Forward proxy

□ Enable upstream proxy (dependent mode)
Proxy server:
Port:

□ Enable guest account
Port number: 8083

□ Enable transparency
○ Use simple transparency
○ Use Web Cache Coordination Protocol (WCCP)
Router IP address(es):
Use a comma "," to separate multiple addresses
Password: (Uses password security)

WCCP Forwarding Method: ○ GRE (Generic Routing Encapsulation)
○ L2 (Layer 2)

○ Reverse proxy
Protected server:
Port: 80

□ Enable SSL Port
Port Number: 443

○ ICAP

□ Enable "X-Virus-ID" ICAP header
□ Enable "X-Infection-Found" ICAP header

FIGURE E-1 Proxy Scan Settings page

Squid Proxy Downstream Mode

In this mode, end-user can receive the content caching on the box and improve the performance. Each client must configure IWSVA device as their proxy server in their browser's Internet connection settings.

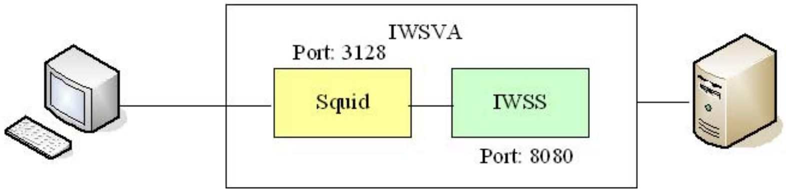


FIGURE E-2 Enable Squid Proxy Downstream

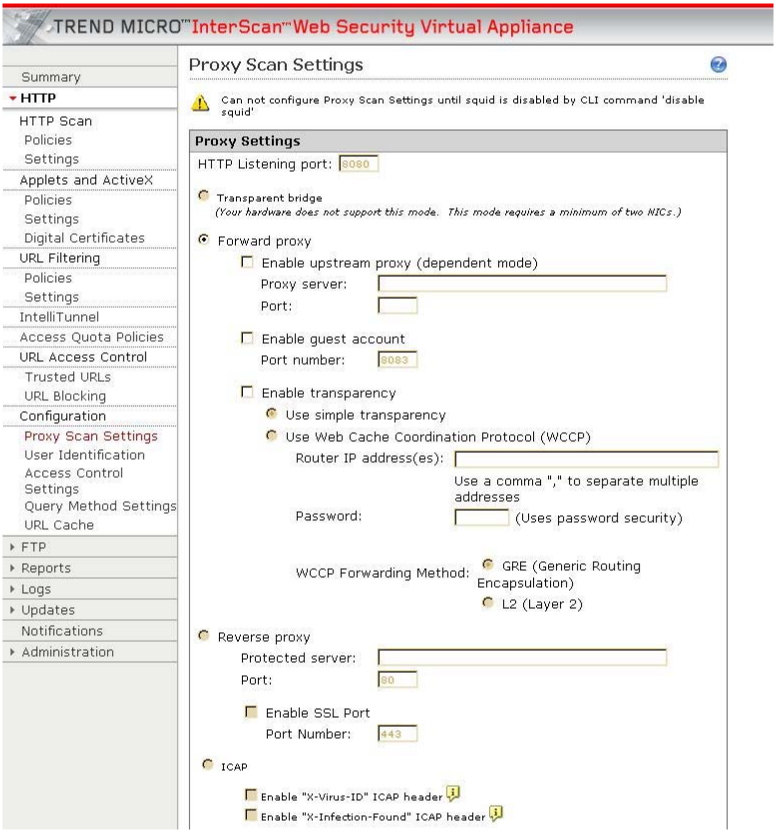
To configure the Squid Proxy Downstream mode:

1. Login IWSVA CLI console as `enable`.
2. Type the following commands:

   ```
   enable squid proxy downstream
   ```

3. Each client on your network needs to configure Internet connection settings to use IWSVA device and port (default 3128) as their proxy server.

Note: If you configure IWSVA to work in Squid Proxy Downstream mode, on the **HTTP > Configuration > Proxy Scan Settings** page of the Web Console, you will not be able to change the HTTP Listening port — the **HTTP Listening port** field will be disabled. See the figure below.



Proxy Scan Settings

Can not configure Proxy Scan Settings until squid is disabled by CLI command 'disable squid'

Proxy Settings

HTTP Listening port: 8080

○ Transparent bridge
(Your hardware does not support this mode. This mode requires a minimum of two NICs.)

● Forward proxy

□ Enable upstream proxy (dependent mode)
Proxy server:
Port:

□ Enable guest account
Port number: 8083

□ Enable transparency
○ Use simple transparency
○ Use Web Cache Coordination Protocol (WCCP)
Router IP address(es):
Use a comma "," to separate multiple addresses
Password: (Uses password security)

WCCP Forwarding Method: ○ GRE (Generic Routing Encapsulation)
○ L2 (Layer 2)

○ Reverse proxy
Protected server:
Port: 80

□ Enable SSL Port
Port Number: 443

○ ICAP

□ Enable "X-Virus-ID" ICAP header
□ Enable "X-Infection-Found" ICAP header

FIGURE E-3 Proxy Scan Settings page with warning message

If you configure IWSVA to work in Squid Proxy Downstream mode, Squid is between the client and IWSS daemons. The IP address presented to the IWSS daemon is that of the Squid process, not the IP address of the client. Therefore, there are following limitations:

- IWSVA cannot use the IP Address user identification method to identify clients or apply policies.

  - When you use LDAP authentication method, after the first client passes the authentication, the other clients using the same proxy setting can pass without authentication.
  - When IWSVA is configured to work with Microsoft Active Directory, the authentication page will not display.
  - To avoid the limitation in IP Address user identification and LDAP authentication when you create HTTP Scan Policies, you can do one of the following:
    - Use only global policy
    - Select accounts only by Host name. See Host Name on page 4-5 for details.
- To avoid the limitation in IP Address user identification and LDAP authentication when you create Access Quota Policies, you can do one of the following:
  - Create a policy using the account of the IP address of Squid process. Then, every client will use the same access quota size.
  - Select accounts only by Host name. Refer to Host Name on page 4-5 for details and its limitation.
- Cannot limit HTTP Access or FTP Access based on the client IP address.
- DCS is unable to connect to a client machine when IWSVA sends the cleanup request.

Squid Proxy Upstream Mode

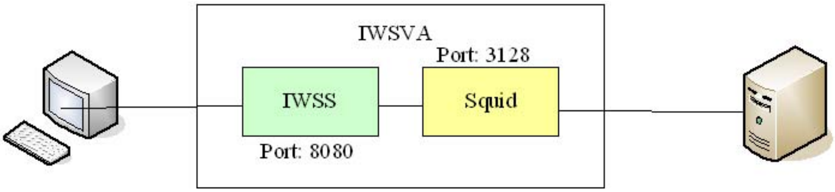


FIGURE E-4 Enable Squid Proxy Upstream

This deployment mode will help the policy enforcement in your network, but will not improve the performance. Each client must configure the IWSVA device as their proxy server in their browser's Internet connection settings.

Note: When you configure IWSVA to work in Squid Proxy Upstream mode, the Server IP Approved List does not take effect. Content from servers that you configure on the Server IP Approved List still will be scanned or filtered.

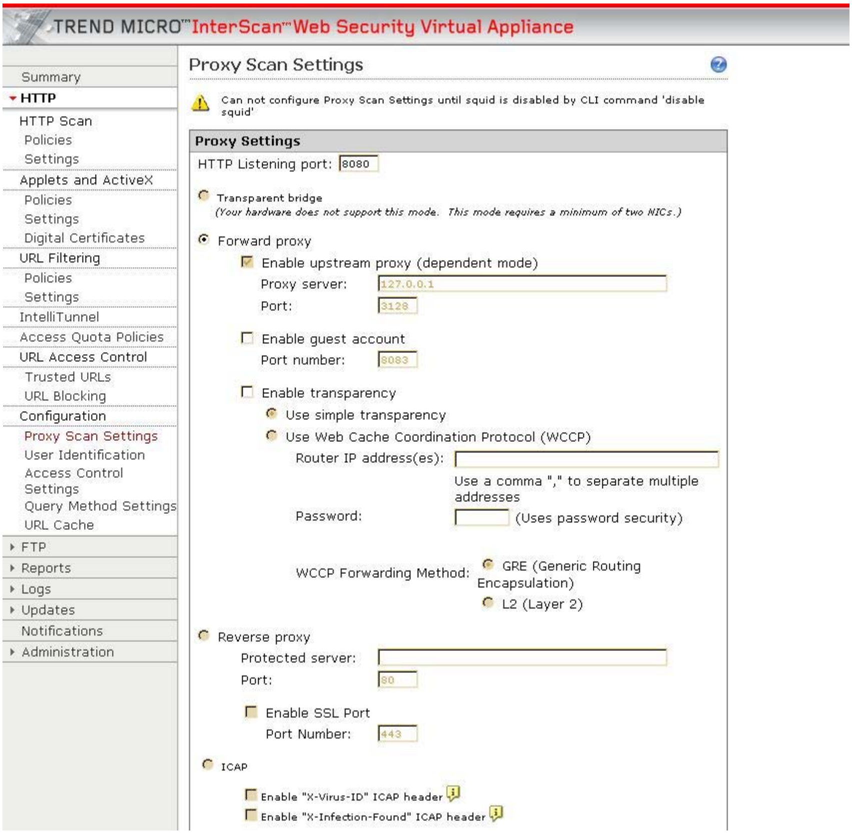
To configure the Squid Proxy Upstream mode:

1. Login IWSVA CLI console as `enable`.
2. Type the following command:

   ```
   enable squid proxy upstream
   ```

3. Each client on your network needs to configure Internet connection settings to use the IWSVA device and port (default 8080) as their proxy server.

Note: If you configure IWSVA to work in Squid Proxy Upstream mode, on the **HTTP > Configuration > Proxy Scan Settings** page and **Updates > Connection Settings** page of the Web Console, you will see the Proxy server IP address is 127.0.0.1 and port is 3128. See figures below:



Proxy Scan Settings

⚠ Can not configure Proxy Scan Settings until squid is disabled by CLI command 'disable squid'

Proxy Settings

HTTP Listening port: 8080

○ Transparent bridge
(Your hardware does not support this mode. This mode requires a minimum of two NICs.)

● Forward proxy

☑ Enable upstream proxy (dependent mode)
Proxy server: 127.0.0.1
Port: 3128

□ Enable guest account
Port number: 8083

□ Enable transparency
● Use simple transparency
○ Use Web Cache Coordination Protocol (WCCP)
Router IP address(es):
Use a comma "," to separate multiple addresses
Password: (Uses password security)

WCCP Forwarding Method: ● GRE (Generic Routing Encapsulation)
○ L2 (Layer 2)

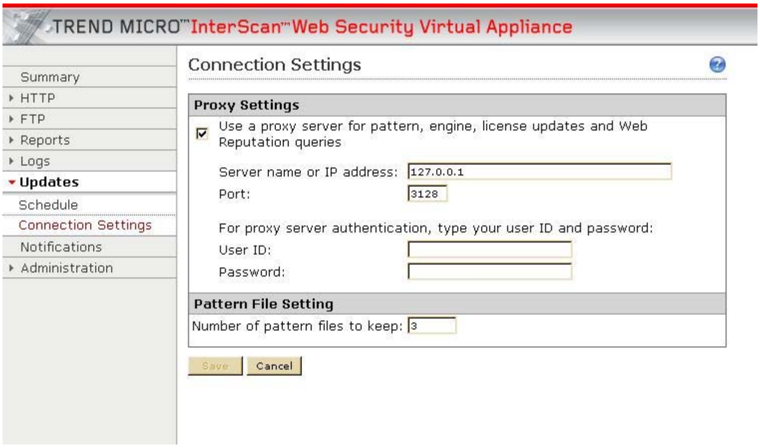
○ Reverse proxy
Protected server:
Port: 80

□ Enable SSL Port
Port Number: 443

○ ICAP

□ Enable "X-Virus-ID" ICAP header
□ Enable "X-Infection-Found" ICAP header

FIGURE E-5 Proxy Scan Settings page with connection settings



Connection Settings

Proxy Settings

☑ Use a proxy server for pattern, engine, license updates and Web Reputation queries

Server name or IP address: 127.0.0.1

Port: 3128

For proxy server authentication, type your user ID and password:

User ID:

Password:

Pattern File Setting

Number of pattern files to keep: 3

FIGURE E-6 Proxy Scan Settings page with proxy settings

Note: When you configure IWSVA to work in Squid Proxy Upstream mode or Squid Proxy Downstream mode, you may find that some HTTPS sites are blocked because Squid has its default access control list, and Squid only allows port 443 as safe HTTPS port by default. Even if you configure IWSVA access control list to allow a HTTPS site which is not using port 443, the site is still blocked by Squid proxy.

Clearing the Squid Cache

Squid is a high-performance proxy caching server for web clients. Sometimes you will need to clear the contents in the cache, to avoid the client from accessing the cached content.

To clear the Squid cache:

1. Login IWSVA CLI console as `enable`.
2. Type the following command:

```
admin squid vacuum
```

Disable Squid service

When you configure IWSVA to work in Squid Proxy Upstream mode or Squid Proxy Downstream mode, IWSVA is not allowed to switch to Transparent Bridge mode, ICAP mode or Reverse Proxy mode. If you want to change IWSVA's deployment mode, you will have to disable Squid service first.

To disable the Squid service:

1. Login IWSVA CLI console as `enable`.
2. Type the following command:

```
disable squid
```

Verifying the Squid Service

Once squid is configured there are a couple of ways to verify that the squid process is in operation.

The first is to configure a browser to use the new squid process. Once this is performed, at the IWSVA CLI, perform the following command:

```
monitor squid
```

Next, initiate traffic through IWSVA. You will notice that in the IWSVA CLI that the access requests will be logged by IWSVA. To stop the logging, use CTRL+C.

Squid Support

The best place to obtain squid support from is the excellent resource `http://wiki.squid-cache.org`. Here you will find good documentation and information to aid with any questions or issues you may have regarding using Squid within your environment.

Trend Micro Disclaimer: Trend Micro IWSVA pre-installs Squid to help reduce the complexity of installing and configuring Squid to function with IWSVA. Squid is disabled by default and must be enabled by the customer through the IWSVA CLI after installation has been completed. Support for Squid is obtained through open source channels and it is the responsibility of the customer to become acquainted with Squid's benefits and functionality before enabling.

Additional information, documentation, and support on the Squid application can be found at the official Squid Web Proxy Cache Web site: `www.squid-cache.org`. Trend Micro will not provide support for Squid's features, but will provide support for the setup and integration of Squid and IWSVA through its CLI commands.

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.
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.
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.

TERM	EXPLANATION
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.
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.

TERM	EXPLANATION
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.
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.

TERM	EXPLANATION
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.
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.
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.
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.

TERM	EXPLANATION
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.
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.
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.

Term	Explanation
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*
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.
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.

TERM — EXPLANATION

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.

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.

Term	Explanation
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
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.
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.

TERM	EXPLANATION
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.
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.
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.

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.

Term	Explanation
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.
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.

TERM	EXPLANATION
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.
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.

TERM	EXPLANATION
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.
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.

TERM	**EXPLANATION**
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.
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.

TERM	EXPLANATION
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.
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).
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).

TERM	EXPLANATION
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.
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 (InterScan Web Security 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.

TERM	EXPLANATION
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.
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.

Term	Explanation
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.
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.

Term	**Explanation**
server farm	A server farm is a network where clients install their own computers to run Web servers, email, or any other TCP/IP based services they require, making use of leased permanent Internet connections with 24-hour worldwide access. Instead of expensive dedicated-line connections to various offices, servers can be placed on server farm networks to have them connected to the Internet at high-speed for a fraction of the cost of a leased line.
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.
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.
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.

TERM	EXPLANATION
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.
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.
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.
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).

Term	Explanation
Total Solution CD	A CD containing the latest product versions and all the patches that have been applied during the previous quarter. The Total Solution CD 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).
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.

TERM **EXPLANATION**

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.

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.

TERM	EXPLANATION
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.
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.

TERM	EXPLANATION
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.
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.

TERM	EXPLANATION
Web server	A server process running at a Web site which sends out Web pages in response to HTTP requests from remote browsers.
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