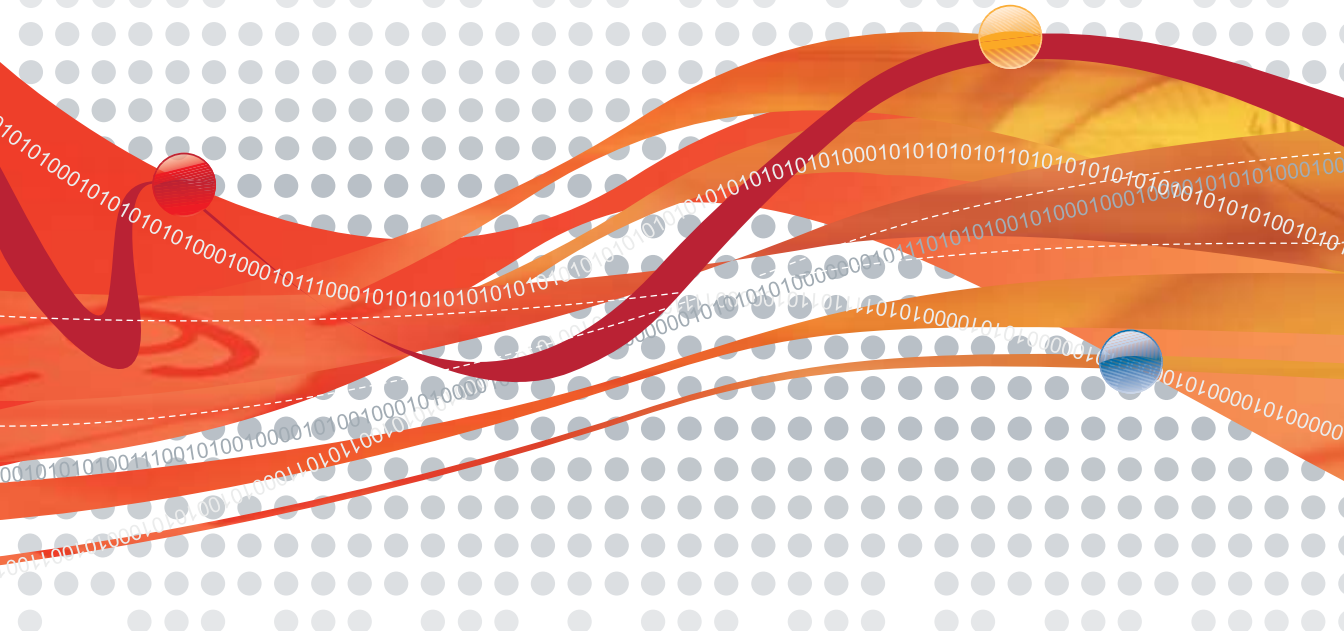
TREND MICRO™

InterScan™ Web Security Suite 3

Antivirus and Content Security at the Web Gateway

for Windows™

Administrator's Guide



Web Security

Release Date: May 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

Welcome to the *Trend Micro™ InterScan Web Security Suite Administrator's Guide* for release 3.1 of InterScan Web Security Suite (IWSS) for Windows. This guide provides detailed information about all IWSS 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:

IWSS Documentation

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

- **Installation Guide** (with deployment information)—this guide helps you get "up and running" by introducing IWSS, assisting with installation planning, implementation, and configuration, and describing the main post-installation 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 IWSS management 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 InterScan Web Security Suite documentation is written for IT managers and email administrators in medium and large enterprises. The documentation assumes that the reader has in-depth knowledge of email messaging networks, including details related to the following:

- SMTP and POP3 protocols
- Message transfer agents (MTAs)

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.

Document Conventions

To help you locate and interpret information easily, the IWSS documentation uses the following 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 Suite

This chapter explains the following:

What's New

This section describes the new features found in InterScan Web Security Suite 3.1 for Windows.

Web Reputation

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

Web Reputation also assigns reputation scores to URLs. For each accessed URL, IWSS 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.

IWSS 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.) IWSS also enables you to monitor the effectiveness of Web Reputation without affecting existing Web-access policies. Results are located in the **URL Blocking Log** or the **Summary** page (**Security Risk Report** tab).

For more Web Reputation information, see *Specifying Web Reputation Rules* on page 6-2 and *Web Reputation Settings* on page 6-3.

Anti-phishing and Anti-pharming Based on Web Reputation

IWSS 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).

Configurable Deferred Scanning

IWSS supports deferred scanning, whereby part of a requested HTTP page is passed to the browser while scanning is in progress to prevent the browser from timing out. When deferred scanning is enabled, IWSS will drop the connection if it detects malware.

Easier Collection of System Information for Support Diagnosis

You can now 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 IWSS system information at the click of a button. See online help for complete details.

True File-type Blocking Within Compressed Files

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

IntelliTunnel

IWSS 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 Notes* on page 4-24.

Direct URL Filter Category Selection

From the Web Reputation database, IWSS 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 more at *URL Filtering Settings* on page 8-4.

Real-time Statistics and Alerts

IWSS provides dynamic statistics where the administrator can view the "real-time" information about the IWSS 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 (a static statistic, updated when the page is opened)
- Bandwidth
- Concurrent Connections
- CPU Usage
- Physical Memory Usage

For more information, see *Real-time Reports* on page 14-5.

Configurable Threshold Warning

You can now set a warning when virus and spyware traffic, database and hard disk size, or bandwidth utilization exceeds a specified threshold. For more information, see *Enabling Threshold Alerts Notifications* on page 13-11.

ICAP Mode Switch

Previously, IWSS 2.5 can be configured to operate in ICAP mode only during installation. Now in IWSS 3.1, you can easily set IWSS to operate in ICAP mode in the Web console.

AAxS Whitelist

IWSS 3.1 supports Java Applet ActiveX Security (AAxS). You can type approved URLs for "Exception to Applet and ActiveX restrictions" in the Web console (**HTTP > Applets and ActiveX > Settings**).

FTP Proxy Enhancements

FTP scanning can be optionally configured to scan uploads and/or downloads. In addition, FTP traffic can be scanned for spyware/grayware, and access control lists can be configured to control access to FTP servers based upon client IP address, server IP address or destination port.

X-Authenticated ICAP Headers Support

IWSS 3.1 supports X-Authenticated ICAP headers that are provided by ICAP clients supporting the ICAP 1.0 protocol. The X-Authenticated headers are available 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 IWSS and second, it allows ICAP clients to provide LDAP searches on LDAP servers with different schemas.

Additional Reporting Information

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

- **Summary > Security Risk Report:** 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
  - Most blocked URLs by user

IWSS reports IntelliTrap activity in the following areas:

- **Summary > Security Risk Report:** Files detected by IntelliTrap are counted as a separate risk in the report.
- **Summary > Scanning:** Files detected by IntelliTrap are listed in the "Scanning results for" with its frequency.
- **Real-time Report**

For more information, see *Types of Reports* on page 14-2.

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 an increasingly 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. InterScan Web Security Suite is a comprehensive security product that protects HTTP and FTP traffic in enterprise networks from viruses and other risks.

In addition to antivirus scanning, IWSS 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.
- For an additional cost, the URL filtering feature blocks access to Web sites with content prohibited by your organization.

- For an additional cost, 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.

Major InterScan Web Security Suite Benefits

Trend Micro InterScan Web Security Suite offers powerful protection for your organization's HTTP and FTP gateway traffic.

Comprehensive Web Security

InterScan Web Security Suite is designed to block Web-based risks, including viruses, Trojans, worms, phishing attacks, and spyware. These risks attack corporate networks through Web-based email and Web pages that contain hidden malicious code. IWSS protects against these risks by scanning HTTP and FTP traffic—vectors left vulnerable by SMTP security solutions. This dedicated HTTP/FTP solution delivers better security and faster throughput, for an improved Web browsing experience.

Centralized Management and Coordination

IT administrators can easily manage InterScan Web Security Suite along with other Trend Micro products within a centralized management console, Trend Micro™ Control Manager. Control Manager provides a unified view of Trend Micro software installations across the enterprise. Activities can be centrally managed, and policies can be applied to all layers of security at the same time. You can view real-time or scheduled reports with enhanced graphs and charts. The end result: you can deploy an immediate, coordinated response to block any emerging risk.

Scalable and Flexible

InterScan Web Security Suite supports a standalone configuration whereby it acts as a proxy server or integrates with existing proxy servers and ICAP-compliant caching servers from Cisco, Network Appliance, and others. InterScan Web Security Suite also supports several LDAP directories, enabling IT managers to set policies and

assign rules for single PCs or groups. You can schedule and automate routine tasks such as pattern file and URL filtering engine updates.

Anti-Spyware/Grayware

Trend Micro's anti-spyware technology is designed to block spyware and adware, plus hacking and remote access tools that could harm the network. This added security helps prevent intruders from collecting personal or corporate information, passwords, email addresses, and other data. It also frees system resources and available bandwidth, improving network performance and reducing spyware-associated system failures (see *About Spyware and Grayware* starting on page 17).

Anti-Phishing and Anti-Pharming

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: Since 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 since 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.

Integration with ICAP 1.0-compliant Caching Devices

Cache servers help moderate Web traffic congestion and save bandwidth. The "retrieve once, serve many" methodology employed by cache servers permits integration with third-party applications such as virus scanning via IWSS. An open

protocol, Internet Caching Acceleration Protocol (ICAP), allows seamless coupling of caching and virus protection.

Leading Virus Protection

Built on Trend Micro's award-winning antivirus technology, InterScan Web Security Suite is serviced 24x7 by the advanced technical team at TrendLabs^{SM}. These engineers monitor virus activity, deliver outbreak prevention policies, and provide updated pattern files, which helps companies minimize outbreak-related costs and damage.

Web Cache Coordination Protocol (WCCP)

IWSS supports the Web Cache Coordination Protocol (WCCP 2.0), a protocol defined by Cisco Systems. The same limitations listed for simple transparency also apply to WCCP transparency, with the exception that FTP connections work and downloads via FTP are scanned. The benefits of WCCP transparency are support for multiple routers and automated reconfiguration for load balancing on router(s) when adding or removing IWSS servers.

Main Features

The following InterScan Web Security Suite features help you maintain HTTP and FTP gateway security.

HTTP Virus Scanning

IWSS 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 InterScan Web Security Suite scans compressed and large files to prevent performance issues and browser timeouts. In addition, InterScan Web Security Suite scans for many types of spyware, grayware, and other risks.

Applets and ActiveX Security

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

In addition, IWSS 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 IWSS, you can set policies based on categories of URLs, such as "Adult", "Gambling," and "Financial Services." When a user requests a URL, IWSS 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.

Access Quota Policies

To set limits on client Web browsing, InterScan Web Security Suite 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

InterScan Web Security Suite can reduce your server's scanning workload by not scanning content trusted URLs. Likewise, InterScan Web Security Suite 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

InterScan Web Security Suite 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 InterScan Web Security Suite, 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.

FTP Scanning

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

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

Reports and Logs

To provide current information about your HTTP and FTP gateway security, IWSS is pre-configured to generate many types of blocking-event reports, traffic reports, spyware/grayware reports, and cleanup reports. 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.

Notifications

InterScan Web Security Suite can issue several types of notifications in response to program or security events. Administrator notifications are sent via 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, InterScan Web Security Suite can also issue notifications as SNMP traps.

Support for Multiple InterScan Web Security Suite Installations

The method to fully administer multiple IWSS servers from a single console is done through Control Manager.

When running more than one IWSS, there are a few things you need to know:

1. Deploying multiple IWSS servers with a common database allows IWSS servers to share policies and configurations stored in the database. To share report and log data store in the common database, select **Database only** or **Database and log files** in the **Write logs to** field in **Logs > Settings > Reporting logs** screen.
2. If one instance of IWSS is installed as stand-alone, then all instances in the IWSS cluster must be stand-alone. Likewise, if one instance of IWSS is installed as an ICAP server, then all instances of IWSS in the cluster must also be installed as ICAP servers.
3. Designate one instance of IWSS as "master" and all other instances as "slave" with the server farm option in the **Administration > IWSS Configuration > IWSS Server Farm** screen allows IWSS servers in the same server farm to share

dynamic data stored in memory. Thus, when dynamic data is updated on a slave IWSS server, the slave server synchronizes the update with the master IWSS server which in turn propagate the update to the other slave servers in the server farm.

Note: Dynamic data include temporary blocked lists and the list of client IP addresses suspected of spyware infection.
The master and slave designation settings in the IWSS Server Farm screen allow you to specify only how dynamic data is shared between multiple IWSS servers in a server farm.

4. To have all IWSS servers in a server farm share the same configuration files, install Trend Micro Control Manager. However, each IWSS server will still store its own configuration for the following:
   - Scan options, schedules, and notification messages
   - Proxy server, LDAP, and other settings
   - Update schedules
   - Log in password
   - User ID method
   - Individual scan engine, pattern, and URL Filtering database files

Note: Trend Micro recommends that you use exactly the same settings for all IWSS servers in one server farm.

Trend Micro Technology in IWSS

This section explains IWSS technology and how it protects your network.

Updatable Program Components

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

- **IntelliTunnel signature definition file:** This file contains "signatures" of certain HTTP interactions (such as instant messaging protocols tunneled through HTTP and SSL authentication requests) which you may wish to control. New signature definition files are typically released several times a year as the covered protocols evolve or new types of HTTP interactions are added. See *Creating a New IntelliTunnel Policy* on page 8-9

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

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

ActiveUpdate

ActiveUpdate is a service common to many Trend Micro products. ActiveUpdate connects to the Trend Micro Internet update server to enable downloads of pattern files, the scan engine, and the URL filtering engine.

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.

The Pattern File

The Trend Micro scan engine uses an external data file, called the pattern file, to keep current with the latest viruses and other Internet risks such as Trojans, mass mailers, worms, and mixed attacks. New 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 *ActiveUpdate* on page 1-15 for details) can detect whenever a new pattern file is available at the server, and/or can be scheduled to automatically poll the server every hour, day, week, and so on to get the latest file.

How Scanning Works

The scan engine works together with the 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 pattern file looking for a match.

Some pattern files (such as virus, Spyware, IntelliTrap, and IntelliTrap Exception patterns) 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 IWSS management 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 `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 pattern files on a regular basis (typically several times per week), and recommends configuring a daily 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.

Incremental Updates of the Pattern Files

ActiveUpdate supports incremental updates of the pattern file. Rather than download the entire 7 or 8MB pattern file each time, ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file. This efficient update method can substantially reduce the bandwidth needed to update your antivirus software and deploy pattern files throughout your environment.

PhishTrap 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 PhishTrap pattern file. The PhishTrap pattern file is saved in `\Program Files\Trend Micro\InterScan Web Security Suite\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 telltale signatures and incorporates the information into the spyware/grayware pattern file. The spyware/grayware pattern file, is stored in the following:

```
\Program Files\Trend Micro\InterScan Web Security Suite\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 IWSS management 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 `tmaptn.###` and contains three digits
- `build number`—this represents the patch or special release number and contains two digits

About Spyware and Grayware

In addition to computer viruses, the IWSS pattern files include signatures for many other potential risks. These additional risks are not viruses since 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.

IWSS can be optionally 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 may be tools or commercial software that have legitimate purposes, in addition to having the potential for malicious actions

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 file 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.

The scan engine includes an automatic clean-up routine for old pattern files (to help manage disk space), as well as incremental pattern updates (to help minimize bandwidth).

In addition, the scan engine is able to decrypt all major encryption 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:

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

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 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`

Component Version Information

To know which pattern file, scan engine, URL filtering engine or program 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.

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" through 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.

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, but they cannot harbor viruses, launch executable code, or carry out any known or theoretical exploits. However, this does not mean that they are entirely safe. 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.

Note: For the highest level of security, Trend Micro recommends scanning all files.

About Damage Cleanup Services

IWSS is compatible with Damage Cleanup Services (DCS), a separately available program from Trend Micro that allows you to automate the cleanup and repair of client systems following or in response to spyware, phish, and other Internet threats.

The IWSS - DCS relationship is especially relevant in networks where "outside" machines such as laptops are allowed to join, or where there is no real-time desktop antivirus solution. IWSS, which monitors inbound and outbound HTTP traffic, can detect outbound traffic to known phish, spyware, and Trojan destinations and block them. It is DCS, however, that can automatically perform the clean up and repair of affected systems.

DCS repairs typically include removing the rogue programs "dropped" by the Trojan onto the client system, cleaning up the Windows Registry, and removing malicious code from memory and/or boot sectors.

If DCS is unable to contact or repair the affected system(s), you can have it report back to IWSS, which can then restrict Internet access by redirecting the client's browser to a manual ActiveX DCS clean-up page.

In the "Example Phish" topic below, IWSS is configured to recognize outbound client requests to the bogus URL and prevent access.

How Damage Cleanup Requests Work

If IWSS is registered to a Damage Cleanup Services (DCS) server, a DCS clean-up request is issued under the following conditions:

- Client PC attempts to access a URL classified as Spyware, Disease Vector, or Virus Accomplice by the PhishTrap pattern or
- Client PC uploads a virus classified as a “worm.”

DCS connects to the client in order to clean the infected file.

IWSS Architecture

InterScan Web Security Suite includes several required and optional modules, depending upon the functions used. The following summarizes the main modules and services. Additionally, many types of scheduled tasks are set up during installation.

IWSS Modules

The following are the main InterScan Web Security Suite modules:

- **Main Program:** Installs the management console and the basic library files necessary for InterScan Web Security Suite.
- **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 InterScan Web Security Suite:** Installs the files necessary for the Control Manager agent to enable monitoring and configuration through Control Manager.

Main Services

IWSS uses the following services:

- **Trend Micro InterScan Web Security Suite Console** (`tomcat5.exe`): This service is the Web server hosting the Web management console.
- **Trend Micro InterScan Web Security Suite for FTP** (`iwssd.exe`): This service enables the FTP traffic flow and FTP virus scanning.
- **Trend Micro InterScan Web Security Suite for HTTP** (`iwssd.exe`): This service enables the HTTP traffic flow and HTTP scanning (including FTP over HTTP). It also handles Applets and ActiveX security processing.

- **Trend Micro IWSS Log Import** (`logtodb.exe`): This service writes logs from text files to the database.
- **Trend Micro IWSS Notification Delivery Service** (`isdelvd.exe`): This service handles administrator notifications (via email) and user notifications (via browser).
- **Trend Micro SNMP Service** (`snmpmonitor.exe`): This service sends SNMP trap notifications to SNMP-capable network monitoring devices.
- **Trend Micro Control Manager Service** (`En_Main.exe`): This service permits IWSS configuration and status reporting through Trend Micro Control Manager, if you are using Control Manager.
- **Trend Micro InterScan Web Security Suite for Dashboard** (`metricmanage.exe`): This service collects system resource data to be used in the display of real-time dashboard metrics.

Scheduled Tasks

When installing IWSS, the setup program creates several scheduled tasks.

- **purgefile.exe:** Runs daily at 2:00 A.M. to delete old text log files, subject to the configured time interval to retain logs.
- **schedulereport.exe:** Runs hourly to check if a scheduled report is configured to run.
- **schedulepr_update.exe:** Runs daily to check if it is time to update the product registration/license.
- **schedule_au.exe:** Runs every 15 minutes to check if it is time to update the pattern file or other program components.
- **cleanfile.exe:** Runs hourly, to remove temporary files downloaded for scan-behind or large file scanning.
- **DbOldDataCleanup.exe:** Runs daily at 2:05 A.M. to clean up old reporting log data in the database and cleans up the old access quota counters in the database.

Chapter 2

Getting Started with IWSS

This chapter explains the following:

Getting Started Checklist

For IWSS requirements, see the *IWSS 3.1 Installation Guide*.

See Table 2-1 for a checklist of tasks to perform after installing IWSS.

TABLE 2-1. Getting Started Checklist

Item	Reference
Learn the Basics	
Learn how to use the Web console	*Opening the IWSS Web Console* on page 2-4
Understand the default settings	*Default Post-install Configuration Settings* on page 2-5
Learn how polices work	*Policy Primer* on page 4-1
Get IWSS Up and Running	
Verify that IWSS Proxy Scan Settings are correct.	*Configuring Proxy Scan Settings* on page 2-8
Configure Update-related proxy settings.	*Proxy Settings for Updates* on page 3-2
Update IWSS components and keep your protection up to date.	*Updating IWSS* on page 2-8
Verify that HTTP traffic flow is enabled.	*Verifying that HTTP Traffic Flow is Enabled* on page 2-9
Test IWSS with the ICAR Test Virus	*Testing IWSS with the EICAR Test Virus* on page 2-9
Protect Your Network	
Configure the User Identification Method that IWSS uses to figure out which of your policies will apply to which clients.	Chapter 5
Configure any of the following policies: • **HTTP Scanning** • **Applets and ActiveX** • **URL Filtering** • **IntelliTunnel** • **Access Control Policies**	Chapter 6 through Chapter 10

Item	Reference
Configure FTP Scanning.	Chapter 10
In addition to the getting started steps, you can also do the following: Use reports and logs. **• Perform administrative tasks on IWSS, such as modifying the Quarantine directory and modifying Database settings.** **• View your product license.**	Chapter 12

Opening the IWSS Web Console

You manage IWSS using the IWSS Web console.

To open the IWSS Web console on a local machine:

Open the Web browser and type the following in the **Address** field:

```
http://localhost:1812
```

To open the IWSS Web console remotely:

Open a Web browser and then type one of the following in the **Address** field:

- `http://<machine name>:1812/index.jsp`
- `http://<IP address>:1812/index.jsp`

See *Accessing the IWSS Console via HTTPS* on page 12-5 for information on how to access the IWSS console using HTTPS.

Logging into the Web Console

Below is the default information that you need to open the IWSS Web console. This information is case-sensitive.

Username — `admin`

Password — `adminIWSS85`

Tip: Change your password regularly.

Default Post-install Configuration Settings

The following table summarizes the default post-install IWSS settings:

TABLE 2-2. Default Post-install IWSS Settings

Feature	Default Post-Install Settings
General settings	• HTTP traffic is on • FTP traffic is on • HTTP and FTP virus scanning, Java applets and ActiveX security, URL blocking and URL filtering are all enabled • Guest account is disabled (thus all guest policies are disabled) • IP address identification method is enabled • Quarantine folder is set to `{install directory}\quarantine`
HTTP virus scanning	The default global and guest policies are configured as follows: • No files are blocked • All files are scanned **Compressed file scanning settings**: The following compressed files are blocked: • Containing more than 50,000 files • Decompressed file size greater than 200MB • More than 10 compressed layers **Large file scanning**: • Files greater than 2048MB are not scanned • Files greater than 512KB are scanned using scan before delivering **Virus scanning actions**: • Infected files are cleaned • Uncleanable files are deleted • Password-protected files are passed • No special action for files containing macros **Miscellaneous settings**: • Quarantined files are encrypted • No special scanning for spyware/grayware

TABLE 2-2. Default Post-install IWSS Settings

Feature	Default Post-Install Settings
Java applet security rules and settings	**Signature validation**: • Valid signature, trusted certificate: Applet is passed • Valid signature, blacklisted certificate: Applet is blocked • No signature: Applet is instrumented • Invalid signature: Applet is blocked • Applet signatures are validated by checking expiration of signing certificate • Certificates that cannot be verified as trusted have their signatures stripped **Allowed applet operations**: • Connecting to originating servers **Disallowed applet operations**: • Destructive and non-destructive operations • Writing or reading data to local disks • Binding to local ports **Miscellaneous**: • Applets cannot create new thread groups • Applets can create active threads (max 8) • Applets can create active windows (max 5) • Applets are left unsigned after instrumentation
ActiveX security rules and settings	• *.cab files, PE files (*.exe, *.ocx): Verify signatures and block blacklisted and block unprocessable signatures of cab files and block unprocessable PE files • Expiration of signing certificate is checked
URL filtering policies	• URL filtering is enabled • Global and guest policies block "Adult" (sites related to illegal drugs, violence and racism and adult-oriented content) and "Computer/Harmful"during work and leisure time • Work time defined to be 8:00 to 11:59 and 13:00 to 17:00, Monday to Friday
Access quota policies	• none
URL blocking	• URL blocking is enabled • All URLs in the PhishTrap pattern (phishing, spyware, virus accomplice and disease vectors) are blocked

TABLE 2-2. Default Post-install IWSS Settings

Feature	Default Post-Install Settings
FTP scanning	• FTP scanning is enabled (for both upload and download scanning) • No file types are blocked • All files are scanned **Compressed file scanning settings**: The following compressed files are blocked: • Containing more than 50,000 files • Decompressed file size greater than 200MB • Containing more than 10 compressed layers **Large file scanning**: • Files greater than 1024MB are not scanned • Deferred scanning is enabled for files greater than 128KB **Miscellaneous**: • Quarantined files are encrypted • No scanning for spyware/grayware • Infected files are cleaned if possible, otherwise deleted • Password-protected files are passed • No special action against macro-containing files
Reports and Logs	• Daily, weekly and monthly consolidated reports for all users are enabled • Reporting logs are written to the database only and kept for 30 days • Reporting logs include performance data • System logs are written to the {install directory}\log folder, and kept for 5 days
Updates	• Check for virus, spyware, and PhishTrap pattern updates weekly • Check for scan engine updates weekly • Check for URL filtering engine updates weekly
Notifications	**Enabled email notifications**: • HTTP file blocking events • URL blocking events • Virus, PhishTrap, spyware pattern updates and URL filtering engine (both successful and unsuccessful) **Disabled email notifications**: • HTTP scanning events • Malicious Java applet and ActiveX events • FTP notifications are on by default • Threshold alerts are on by default
Damage Cleanup Services	• Client browsers are redirected to DCS if cleaning fails

Note: For large file handling, IWSS 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 enables or JavaScript disabled, then the progress page does not function and scanning is prevented.

In order for the progress page to work, IWSS needs to know to which externally visible IP address the clients will 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` (for example, `iscan_web_server=1.2.3.4:1812`) or modify the `hosts` file so that the host name does not resolve to 127.0.0.1.

Configuring Proxy Scan Settings

IWSS is in **Forward Proxy (Standalone)** mode by default. The type of proxy can be modified in the IWSS console, along with several other proxy-related settings such as the email address for anonymous FTP logon over HTTP, the number of threads, and the number of concurrent connections to the IWSS server.

To modify your proxy settings:

1. Click **HTTP** > **Configuration** > **Proxy Scan Settings** from the main menu.
2. On the **Proxy Settings** page, review the existing configurations and modify if necessary.

Updating IWSS

Now that IWSS is connected to the Internet, you must update its components to protect your network from the latest threats.

To manually update:

1. Click **Summary** in the main menu.
2. On the **Scanning** tab of the **Summary** page, select the component to update and click **Update**. A progress bar displays to indicate the update progress, and a message screen displays the outcome of your update attempt.

Verifying that HTTP Traffic Flow is Enabled

After installing IWSS, the HTTP service is enabled by default. The HTTP traffic flow for your clients to browse the Web and perform other HTTP operations can be turned on or off.

To verify that HTTP traffic flow is enabled:

1. Click **Summary** on the main menu.
   If the **Turn On** link already appears, do not click it.
2. If HTTP traffic is turned off, click **Turn On**.

Testing IWSS with the EICAR Test Virus

The European Institute for Computer Antivirus Research (EICAR) has developed a test virus to test your antivirus software. This script is an inert text file. The binary pattern is included in the pattern file from most antivirus vendors. The test virus is not a virus and does not contain any program code.

WARNING! *Never use real viruses to test your antivirus installation!*

Obtaining the EICAR Test File

Download the EICAR test virus from the following URLs:

`http://www.trendmicro.com/vinfo/testfiles/`

`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 cache in the cache server 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, thus IWSS would not detect the file.

Chapter 3

Updates

This chapter explains the following:

Proxy Settings for Updates

If you use a proxy server to access the Internet, you must enter the proxy server information into the IWSS management console before attempting to update. 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 IWSS management 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 InterScan Web Security Suite server 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, for example, excessive false positives. When the number of pattern files on the server exceeds your configuration, the oldest pattern file will be automatically deleted.
5. Click **Save**.

Updating Manually

To manually update:

1. Click **Summary** in the main menu.
2. On the **Scanning** tab of the **Summary** page, select the component to update and click **Update**. A progress bar displays to indicate the update progress, and a message screen displays the outcome of your update attempt.

Forced Manual Updates

IWSS provides an option to force an update to the pattern file and the scan engine when the version on the IWSS server is greater than or equal to its counterpart on the remote download server (normally IWSS 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** in the main menu.
2. Select the component to update and then click **Update**. A message box displays if the version of the pattern file or scan engine on the IWSS server is greater than or equal to the counterpart on the remote download server.
3. Click **OK** in the message box to start the forced update.

Scheduling Updates

To schedule automatic pattern file, scan engine and URL filtering engine updates:

1. Click **Updates > Schedule** from 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 scan engine and URL filtering engine updates)

Note: Scheduled updates for a given component can be disabled by selecting **Manual updates only** under the components 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 IWSS management console to verify the current version of the pattern file. Trend Micro recommends that you flush the cache and reboot the NetCache appliance and Blue Coat Port 80 Security Appliance after updating the pattern file to ensure that no viruses are being cached. Consult your Netcache appliance and your Blue Coat Security Appliance documentation for instructions on how to clear the cache and reboot.

Maintaining Updates

Verifying a Successful Update

The **Scanning** tab of the **Summary** page in the IWSS management console displays the version of the component in use, plus the modification time and the date the pattern file was last updated. Check the **Summary** page to verify that a manual or scheduled update has completed successfully.

Update Notifications

IWSS can issue notifications to proactively inform an administrator about the status of a pattern file, URL filtering engine or scan engine update (see *Notifications* on page 13-1).

Rolling Back an Update

IWSS 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 may incorrectly detect a non-infected file as a virus infection (known as a "false alarm"). You can revert to the previous pattern file or engine library file.

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

1. Click **Summary** in the main menu. The **System Dashboard** tab displays 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.

Note: Rollbacks are only supported for the pattern file and virus scan engines, and only for registered versions of IWSS.
IWSS does not support rollback for the URL filtering engine.

Deleting Old Pattern Files

After updating the pattern file, IWSS keeps old pattern files on the server so they are available for rollback. 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 `{install directory}\` directory of IWSS.

Controlled Pattern File Releases

There are two release versions of the Trend Micro 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 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.

To apply the latest CPR to IWSS:

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 IWSS server. The file name will be in the form lptXXX.zip.
3. Stop all the IWSS services.
4. Extract the contents of the files that you downloaded to the `{install directory}\` directory of IWSS.
5. Restart all IWSS services.

To verify that the CPR was applied correctly, click **Summary** in the main menu and confirm that the pattern file version in use corresponds to the version of the CPR that you tried to apply.

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

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

Chapter 4

Policy Primer

This chapter explains the following:

How Policies Work

Different security settings can be configured for different users or groups on your network, based on the type of files or Internet resources they need to access.

Note: Before creating policies, verify that you correctly configured the user identification method (the way IWSS identifies clients on your network). For instructions, see *Understanding the User Identification Method* on page 4-4.

Policies are classified as follows:

- **HTTP scanning for viruses and Spyware/Graywere:** Your organization's acceptable use policy may generally prohibit clients from downloading audio or video files. However, there may 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.

  For more information, see See *HTTP Scanning Notes* on page 4-16.

- **Java Applets and ActiveX security:** To prevent clients from running applets that could intercept sensitive information and transmit it over the Internet, you may 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.

  For more information, see See *Java Applet and ActiveX Security Notes* on page 4-18.

- **URL filtering:** To discourage your employees from engaging in non-work-related Web surfing, you may 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.

  For more information, see See *URL Filtering Notes* on page 4-22.

- **IntelliTunnel:** IWSS enables you to block communication provided by certain Instant Message (IM) protocols and certain authentication connection protocols.

  For more information, see See *IntelliTunnel Notes* on page 4-24.

- **Access quotas:** IWSS allows you to configure access quota policies to limit the volume of files that clients can download during the course of a 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.

  For more information, see *Access Quotas and URL Access Control* on page 9-1.

Default Global and Guest Policies

InterScan Web Security Suite has the following default policies for all policy types.

- **Global Policy**: For all clients who access IWSS through the **Listening port number** (default port = 8080).
- **Guest Policy**: For clients, typically temporary workers, contractors and technicians who access IWSS through a special guest port (default port = 8081).

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

Configure both policies by choosing **HTTP > Configuration > Proxy Scan Settings** from the main menu.

About the Guest Policy

The guest port is a feature that's available when the administrator has configured IWSS to run in HTTP 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 don't have accounts in the directory server, for example, contract personnel or visiting vendors, can still access the Web. The default port values are 8080 for users in the directory, and 8081 for guests. The Guest Policy is the only policy applied to guests.

For more information about enabling the "User/group name" user identification method, see See *Using Group User or Group Names* on page 4-6.

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 IWSS reads the information from the database after the time intervals specified under **Policy Deployment Settings (in minutes)** on the **Administration > IWSS 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 will be interrupted for a short time (ten seconds).
In the IWSS default setting, the LDAP cache is refreshed in IWSS in 1.5 hours. Therefore, if you modify your directory, such as moving one user to another group, the refresh might not take effect in IWSS immediately.

Understanding the User Identification Method

In order to define the scope of HTTP virus scanning, URL filtering, Applets and ActiveX security, IntelliTunnel security, and access quota policies, configure how IWSS will identify clients. Your choice of user identification method also determines how security events are traced to the affected systems in the log files and reports.

IWSS provides the following user identification methods to identify clients and apply the appropriate policy:

- No identification (does not identify the client machine for HTTP requests)
- IP address (default option)
- Host name (modified HTTP headers)
- User/group name via proxy authorization (LDAP)

Using No Identification

The **No identification** option is used when an administrator does not want the client machine names to be reviewed for traffic via HTTP. The type is Unknown for this option, and can be found under the User ID column in various logs.

IP Address

The IP address is the default identification option and requires the following:

- Client IP addresses are not dynamically assigned via DHCP
- Network address translation (NAT) is not performed on the network path between the affected system and IWSS

Use IP addresses for identifying users if all of the following are true:

- Each person in the organization is assigned his or her own client computer
- Each client computer is assigned its own, static IP address
- Each client computer is secure from use by other

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.

Host Name

Identifying users by host name requires that IWSS perform an additional step. IWSS does a hostname lookup on the source IP address of each HTTP proxy request.

The Host name (modified HTTP headers) option logs the MAC address of the affected machine and Windows machine name to the virus log, URL blocking log, and Internet access log. Choose this option if the access is via Internet Explorer on Windows. This option requires that you run a Trend Micro-supplied program on each Windows client.

An effective method of deployment 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\Internet Settings\UserAgent\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 where you made the HTTP requests. The use of the MAC address is advisable because of its unique and traceable ID. The machine name is an additional and helpful identifier.

The additional work can make this mechanism slower than using IP addresses. Because the mechanism is still based on IP addresses, it has the following requirements and options:

- Clients use Internet Explorer on the Windows platform
- Meet all the conditions listed for using IP addresses only
  - Each person in the organization is assigned his or her own client machine
  - Each client machine is assigned its own, static IP address
  - Each client machine is secure from use by others
- The administrator must configure each client computer (Windows-based operating systems only) to use extended HTTP request headers which include the MAC address and machine name, using the utility program `register_user_agent_header.exe` found in the `{Install folder}\ieagent\` folder. This program modifies a registry entry used by Internet Explorer. Administrators can perform this task readily by invoking the utility from a Windows domain logon script.
- The administrator can set policies based on individual hostnames

Using Group User or Group Names

The User/Group name method of user identification relies solely on the LDAP database. When using this mechanism, administrators must:

- Configure a supported LDAP server on the network
- Create a user account or record on the LDAP server for each user who will proxy requests through IWSS

Note: IWSS supports using the LDAP database that is part of the Active Directory service on Windows 2000 servers (or above), the Linux OpenLDAP server, or Sun's iPlanet Directory Server.

When using this mechanism, administrators must:

- Configure a supported LDAP server on the network
- Create a user account or record on the LDAP server for each user who will proxy requests through IWSS

While using this mechanism to identify users, administrators can create policies using:

- Individual IP addresses (as with the IP address mechanism)
- Ranges of IP addresses (as with the IP address mechanism)
- LDAP-authenticated users or groups

When administrators configure LDAP as the user identification mechanism, users must enter valid usernames and passwords when their browser first connects to the IWSS HTTP service. Once authenticated, the user remains authenticated for the duration of the browser session.

The User/group name via proxy authorization option verifies the user credentials as well as retrieves the group information. The directory service makes the physical network topology and protocols transparent so that a user on a network can access any resource without knowing where or how it is physically connected. LDAP defines a standard method for accessing and updating information in a directory. The information needed to use a user validation/group retrieval during proxy authorization are as follows:

- LDAP server hostname
- Listening port number
- LDAP admin account
- Password
- Base distinguished name (served as a starting point for LDAP search operation)
- Authentication method (**Simple** to pass the admin password as plain-text or **Advanced** to use the Kerberos/Digest-MD5 authentication, depending on the directory server's vendor)

The authentication behavior between IWSS and the directory server differs from the authentication method used between the client browser and IWSS. The authentication method between client browsers and IWSS is explained in *Table D-1* on page 4-10. User logon authentication remains secure when choosing simple authentication for the user credential that is passed between IWSS and the directory server. This option uses plain text for the LDAP administrator account credential configured on the LDAP settings page, and this credential is passed between IWSS and the directory server for initial LDAP authentication or connection testing only. During user logon, IWSS still uses the advanced authentication method (not revealing a user's password) when sending the users' credentials between IWSS and

the directory server. Secure authentication for the latter depends upon the directory server's vendor, either Kerberos or Digest-MD5.

Notes on User/Group Name via Proxy Authorization

The user/group proxy authorization identification method resolves some of the limitations of other identification methods:

- **IP address:** It is impossible to identify the person making a request if multiple users share the same computer, or if IP addresses do not adequately identify the computer where a request originates
- **Host name (modified HTTP headers):** User/group proxy authorization can be configured in environments where multiple operating systems are used, while the host name identification method only works on Windows for Web browsing via Internet Explorer

User/group proxy authorization operates effectively in environments where:

- Multiple platforms or applications are used
- Machines may be shared between employees, and
- IP addresses are insufficient to uniquely identify source machines

With user/group proxy authorization enabled, you can define policies based on user names and groups rather than IP addresses/ranges and machine names.

With user/group proxy authorization enabled, you can define policies based on user names and groups rather than IP addresses/ranges and machine names.

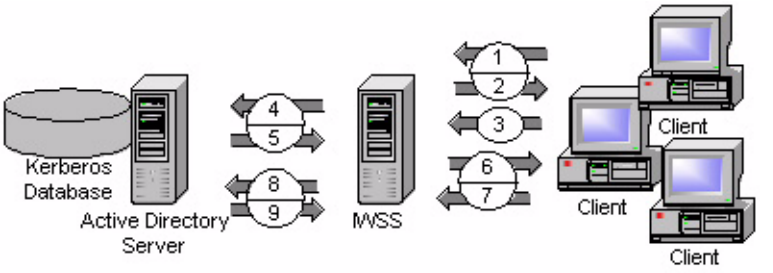


FIGURE D-1. LDAP server authentication workflow (Active Directory shown)

The following steps explain the authentication workflow for Active Directory (AD) shown in Figure D-1. on page 8 Authentication workflow for other directory servers are similar.

1. Client requests a URL.
2. IWSS sends proxy authorization request to client.
3. Clients requests the URL again, and sends handshaking information.
4. IWSS sends handshaking information to Active Directory server.
5. Active Directory server sends handshaking information to IWSS.
6. IWSS sends handshaking information to client.
7. Clients enter proxy authorization credential.
8. IWSS relay user credential to LDAP server.
9. Active Directory server authenticates the user.

After the client authenticates, IWSS forwards the client request to the Web server.

However, proxy authorization also has some drawbacks that must be considered. The primary drawback is *inconvenience* for the end user. IWSS prompts clients to authenticate by providing a username and password. Once these credentials are verified, browsing may commence. Many applications save this information as long as the application remains open, and will attach the credentials with each request. This information, however, is not shared with other applications, including any additional instances of the same application. As a result, clients may need to enter their credential several times.

Additionally, some applications that tunnel over port 80 do not display a pop-up window when challenged and either require the user to set their proxy credentials ahead of time through a configuration setting, or simply do not operate at all when the proxy requires authentication.

Another concern is *security.* IWSS supports Basic and NT LAN Manager (NTLM) authentication techniques when installed in HTTP proxy mode, but only Basic when installed in ICAP mode. Consider the following:

TABLE D-1. Behavior of BASIC and NTLM authentication methods

Behavior	BASIC authentication	NTLM authentication
User name/password	Transmitted in clear text between the browser and IWSS	Uses only hashes to transmit the user's credentials between the browser and IWSS
Active Directory authentication by Kerberos (browser > IWSS > Active Directory server)	User's credentials are vulnerable when passed between the browser and IWSS, credentials are encrypted via Kerberos between IWSS and the Active Directory server	User's credentials are secure when passed between the browser and IWSS, and between IWSS and the Active Directory server
Microsoft applications	New applications will prompt the user to supply credentials. After authentication of an application, additional instances of the same application typically "remember" the credentials and continue to supply them for subsequent requests.	Some applications, such as Internet Explorer, can access the user's credentials without requiring a pop-up window—other applications, such as Mozilla, streaming media players, Java news tickers, and so on will still display pop-up windows Note: NTLM cannot be used in ICAP installations
NTLM application support	IWSS will only issue NTLM challenges to Internet Explorer and versions of Mozilla 1.4.1 and above	

In network environments where IP addresses adequately identify the machines where requests originate, IWSS can use a cache that retains a previously-entered credential for a period of time. The default time-to-live (TTL) for entries in this cache is 90 minutes for both HTTP and ICAP modes.

Note: (1) ICAP mode does not support NTLM and single sign-on, but does support BASIC and IP-based credential caching.
(2) HTTP mode or Dependent mode supports NTLM, BASIC, single sign-on, and IP-based credential cache.

IWSS and LDAP

IWSS can integrate with the following LDAP servers, and supports both the LDAP 2 and three protocols:

- Microsoft™ Active Directory 2000 and 2003
- Linux™ OpenLDAP Directory 2.2.17
- 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:

	Kerberos	Simple authentication	NTLM
Microsoft Active Directory 2000 and 2003	yes	yes	yes
Linux OpenLDAP 2.2.17	yes	yes	no
Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)	no	yes	no

TABLE 4-2. Authentication methods for supported LDAP servers

LDAP Communication Flows

When a client requests Internet content, they are prompted to enter their network credential. Simple authentication sends the network credential via clear text.

Advanced authentication uses a Kerberos server as a central secure password store, thus the benefit of using Kerberos is a higher degree of security. After the client authenticates with Kerberos, a special encrypted "ticket" certified by the Kerberos server is used to access IWSS and the Internet.

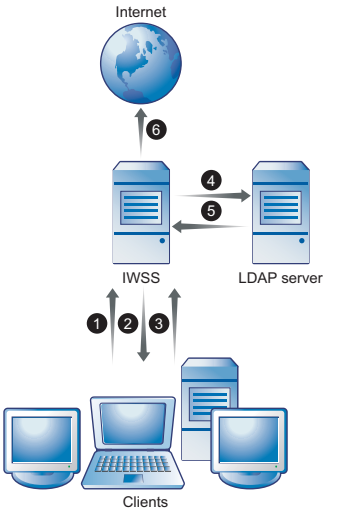


FIGURE 4-2 LDAP communication flow using Kerberos authentication

The following steps explain the authentication workflow for Active Directory (AD) shown in Figure 4-2. Authentication workflow for other directory servers are similar.

1. Client requests a URL.
2. IWSS sends proxy authorization request to client.
3. Clients requests the URL again, and sends handshaking information.
4. IWSS sends handshaking information to Active Directory server.
5. Active Directory server sends handshaking information to IWSS.
6. IWSS sends handshaking information to client.
7. Clients enter proxy authorization credential.
8. IWSS relay user credential to LDAP server.
9. Active Directory server authenticates the user.

After the client authenticates, IWSS forwards the client request to the Web server.

However, proxy authorization also has some drawbacks that must be considered. The primary drawback is *inconvenience* for the end user. IWSS prompts clients to authenticate by providing a username and password. Once these credentials are verified, browsing may commence. Many applications save this information as long as the application remains open, and will attach the credentials with each request. This information, however, is not shared with other applications, including any additional instances of the same application. As a result, clients may need to enter their credential several times.

Additionally, some applications that tunnel over port 80 do not display a pop-up window when challenged and either require the user to set their proxy credentials ahead of time through a configuration setting, or simply do not operate at all when the proxy requires authentication.

Another concern is *security.* IWSS supports Basic and NT LAN Manager (NTLM) authentication techniques when installed in HTTP proxy mode, but only Basic when installed in ICAP mode. Consider the following:

TABLE 4-3. Behavior of BASIC and NTLM authentication methods

Behavior	BASIC authentication	NTLM authentication
User name/password	Transmitted in clear text between the browser and IWSS	Uses only hashes to transmit the user's credentials between the browser and IWSS
Active Directory authentication by Kerberos (browser > IWSS > Active Directory server)	User's credentials are vulnerable when passed between the browser and IWSS, credentials are encrypted via Kerberos between IWSS and the Active Directory server	User's credentials are secure when passed between the browser and IWSS, and between IWSS and the Active Directory server

TABLE 4-3. Behavior of BASIC and NTLM authentication methods

Behavior	BASIC authentication	NTLM authentication
Microsoft applications	New applications will prompt the user to supply credentials. After authentication of an application, additional instances of the same application typically "remember" the credentials and continue to supply them for subsequent requests.	Some applications, such as Internet Explorer, can access the user's credentials without requiring a pop-up window—other applications, such as Mozilla, streaming media players, Java news tickers, and so on will still display pop-up windows Note: NTLM cannot be used in ICAP installations
NTLM application support	IWSS will only issue NTLM challenges to Internet Explorer and versions of Mozilla 1.4.1 and above	

In network environments where IP addresses adequately identify the machines where requests originate, IWSS can use a cache that retains a previously-entered credential for a period of time. The default time-to-live (TTL) for entries in this cache is 90 minutes for both HTTP and ICAP modes.

Note: (1) ICAP mode does not support NTLM and single sign-on, but does support BASIC and IP-based credential caching.
(2) HTTP mode or Dependent mode supports NTLM, BASIC, single sign-on, and IP-based credential cache.

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, IWSS initially searches in 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” will only return “John Smith” and “John Jones” since matching entries exist in the main LDAP server and the search will not extend to the referral servers. However, a query for “John Carter” will extend down to the secondary referral server and return “John Carter Rubin” since 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 IWSS 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 reside 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 IWSS to listen on port 3268, the Microsoft Active Directory server that IWSS 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.

HTTP Scanning Notes

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, may take longer as gateway antivirus software performs virus scanning. Some of the requested files may be large and determining whether the file is safe requires downloading the entire file before it is relayed to the user. Content may 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 due to its MIME content-type, IWSS will attempt 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 will be scanned. Unfortunately, there is not always a clear mapping between file types and MIME types. If IWSS cannot map the true file type to a MIME type, it will be 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 may not accurately represent the true type of the content to download. Secondly, some types that you may think are safe to skip (for example, text) may not really be safe (since scripts are text, and may possibly be malicious). One more area where you may 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 IWSS scan engine will scan all that traffic because the content may 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 may choose to add text/* to your MIME content-type skip list so IWSS 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 will propagate more slowly, because the file containing malicious code will take longer to transmit. Therefore, it is important to screen small files efficiently and completely.

Note: Performance may 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) is invoked more often.

Java Applet and ActiveX Security Notes

IWSS 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.

IWSS employs a tiered technology approach that operates on both the Internet gateway server and on desktops.

- On the server, IWSS 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, IWSS code, inserted into Java applets, monitors the behavior of the applets in real time and determines whether their behavior is malicious according to a pre-configured security policy.

Figure 4-3 on page 18 illustrates how IWSS scans and blocks malicious applets and ActiveX objects.

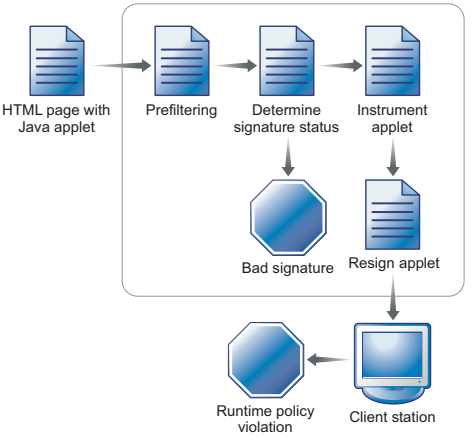


FIGURE 4-3 How Java applet security works

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, IWSS 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, IWSS filters them according to the following criteria:

For ActiveX Objects

If ActiveX security is enabled, IWSS checks the signatures of CAB files and executable COM objects (of which ActiveX controls are a type) that are digitally signed. It will then examine the digital certificates contained in the signature and compare them with those in the IWSS-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.

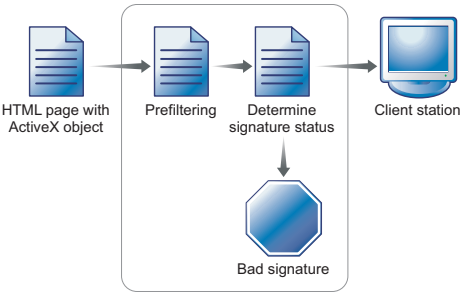


FIGURE 4-4 How ActiveX security works

For Java Applets

IWSS 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, IWSS will verify 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.

IWSS 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.

For Java Applets, IWSS first performs Steps 2 and 3 below before sending the applets to the clients.

Step 2. Instrumenting Java Applets

IWSS analyzes the applet code to determine any potentially dangerous actions that it may 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, IWSS inserts monitoring code around suspicious instructions and then attaches the security policy assigned to the intended recipients. Depending on how IWSS is configured, this security policy may vary from one client to another based on the domain they belong to, or their IP addresses. IWSS supports creating multiple policies that can be mapped to different groups of users in your network. IWSS 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. IWSS can optionally re-sign the applet if required by the client browser.

Step 3. Optionally Re-signing Instrumented Applets

If configured to do so, IWSS re-signs the instrumented applets using an imported "private key" before sending them to client workstations. Since applets lose their original signatures during the instrumentation process (due to modifications to their original code), you may want to use this feature to ensure that the clients' Web

browsers will run the instrumented applets with the permissions they may require to run correctly.

IWSS supports the import of a “private key”, along with the associated certificate that contains the corresponding “public key,” for use in the re-signing process. You can purchase this key from any of the well-known Certifying Authorities (CAs). Only one re-signing key may be configured for use at any given time.

Note: Re-signing applies only to validly signed applets. If the system is configured to accept unsigned applets, these applets will bypass this process and will be 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, IWSS then allows the action to take place. Otherwise, IWSS takes the configured action, which can be one of the following:

- Stop the applet and display a message.
- Notify the users and give them the option to allow the behavior, terminate the behavior, or stop the applet.

URL Filtering Notes

The default settings for the IWSS 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 may be created to allow access to restricted category groups for employees whose job function requires broader access. For example, members of the Human Resources or IT departments may need unrestricted Internet access to conduct investigations into violations of your organization's acceptable Internet use policies.

In addition, IWSS also provides enhancement as it combines dynamic filtering with advanced databases. Browsing Web sites related to online trading, shopping, auction bidding, dating, gambling and other non-work related topics during work time reduces employee productivity and decreases bandwidth available for legitimate browsing. IWSS allows Internet access to be customized according to user and workgroup-specific needs, thus optimizing the use of the Internet.

IWSS allows for very flexible application of the URL filtering policy. There are three basic mechanisms for customization:

- IWSS includes a database that contains URLs in over 60 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 may 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 may 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. IWSS gives you the option to configure 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 IWSS is configured to use (see *Configuring the User Identification Method* on page 5-2).

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.

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. IWSS 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
- Compression ratio exceeds: 99% (Files with less than 99% compression ratio are automatically allowed by IWSS)

Large File Handling

If the delay when downloading large files is unacceptable, IWSS 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. For more information, see See *Deferred Scanning* on page 6-11. 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 IWSS is configured to quarantine files as a scan action, it can optionally encrypt the files to prevent them from being accidentally executed by someone browsing the quarantine folder. Note that once encrypted, the files can only be decrypted by a representative from Trend Micro's Support department.

Scanning for Spyware/Grayware

IWSS 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* on page 6-12.

IntelliTunnel Notes

IWSS can filter HTTP traffic for IM protocols and authentication connection protocols and based on a specified policy, block certain content from entering the LAN. You can create multiple policies to have IWSS apply different filter criteria to different user groups within your organization.

Note: IM/authentication connections policy enforcement is only possible when the IM/authentication connections clients are made to use HTTP tunneling. This requires that the site is set up to allow only external network access via 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 IWSS.

About Instant Messenger Protocols

IWSS can block most services using popular instant messenger protocols, such as ICQ, AOL, MSN and Yahoo Messenger.

Note: IWSS is not able to block direct TCP connections some new versions of MSN/Windows Live Messenger use.

About Authentication Connection Protocols

IWSS can block authentication connection communications that use the following technology:

- **Google Talk** - A full-fledged IM client based on the open Jabber protocol which also includes Voice over Internet Protocol (VoIP). VoIP is a category of hardware and software that enables you to use the Internet as the transmission medium for telephone calls. This technology sends voice data in packets using IP rather than by traditional circuit transmissions of the Public Switched Telephone Network (PSTN).
- **Jabber IM** (jabber.org) - An open XML protocol for message and presence exchange in real time between two points on the Internet. Jabber's asynchronous instant messaging platform is similar to IM systems such as AOL, ICQ and MSN but is open source, extensible through XML, decentralized (allowing anyone to run a Jabber server), and any Jabber server can be isolated from the public Jabber network in order to increase security.

Note: IntelliTunnel does not block Google Talk or Jabber IM in ICAP mode.

Access Quota Policy Notes

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

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.

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.

URL Access Control Notes

InterScan Web Security Suite can control URL 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 IWSS.

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:

- IWSS checks the requested URL against the URL blocking list and trusted URL list.

  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, IWSS 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 IWSS blocks the URL (see *Specifying Web Reputation Rules* on page 6-2).

  If the URL is found on the Web Reputation exception list, IWSS skips the anti-phishing and anti-pharming detection for this URL (see *Specifying Web Reputation Exceptions* on page 6-4).
- Web Reputation then determines if the requested URL is a phishing or pharming threat and if so, flags the URL accordingly.
- The final process of Web Reputation is to determine the category of the URL.

  The category information is used later by the optional URL Filtering module.
- Web Reputation returns to IWSS the URL rating, any phishing or pharming flags, and the URL category.
- If a URL is flagged for phishing or pharming, IWSS 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 8-5).

  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, IWSS determines if 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, IWSS skips the sensitivity level checking for this URL (see *Specifying Web Reputation Exceptions* on page 6-4).

  If the rating falls below the sensitivity level, the requested URL is blocked. However, if the rating is above the sensitivity level, IWSS grants access.

FTP Scanning Notes

InterScan Web Security Suite can scan FTP uploads and downloads for viruses and other malicious code in a similar manner 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.

InterScan Web Security Suite 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 29). 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 a white list so that downloads from them will not be scanned. Moreover, to further lock down the InterScan Web Security Suite server, FTP access to specific ports can either be allowed or denied.

FTP Settings

InterScan Web Security Suite FTP scanning settings include options for using either the IWSS native (stand-alone) proxy or a separate FTP proxy, two options for how data connections are made (active FTP vs. passive FTP) and performance-related settings that control the maximum number of concurrent client connections and processing threads.

Proxy Settings

InterScan Web Security Suite FTP scanning provides two proxy options—a "stand-alone" mode whereby clients connect to the native IWSS proxy that later connects with the FTP server, and an "FTP proxy" mode whereby IWSS 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 IWSS should connect to.

- In FTP proxy mode, no username is required because InterScan Web Security Suite 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 InterScan Web Security Suite FTP scanning module is dedicated to the specified FTP server, in a similar manner to a reverse proxy for HTTP scanning. For more information about InterScan Web Security Suite FTP proxy options, consult the *IWSS Installation Guide*.

Passive and Active FTP

InterScan Web Security Suite 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 InterScan Web Security Suite configuration, InterScan Web Security Suite converts "active" mode on the client side into passive mode on the server side. Mode conversion is performed only when the IWSS configuration is passive and the client uses active mode. If the IWSS configuration is active, no conversion is performed, so passive requests from the client are still passive requests on the server side.

FTP Scan Direction

Depending on how you want to use IWSS 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 may be justified to achieve a performance benefit since 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 manually configure. If your organization has policies that prohibit certain types of files in your network, IWSS 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* on page 1-20for 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.

Chapter 5

Configuring the User Identification Method and the Guest Port

This chapter explains the following:

Configuring the User Identification Method

Configure how IWSS will identify clients:

- IP address (default option)
- Host name (modified HTTP headers)
- User/group name via proxy authorization (LDAP)

IP Address

To enable the IP address user identification method:

1. Select **HTTP > Configuration > User Identification** from the main menu.
2. Under the **User Identification Method** section, check **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.

Note: By default, only the host name portion of the host name/MAC address combination is stored in IWSS logs and used to match policies.

If you want to use both the host name and MAC address for user identification, then 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) since 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.

To enable the Host name identification method:

1. Select **HTTP** > **Configuration** > **User Identification** from the main menu.
2. Check **Host name (modified HTTP headers)**.
3. Click **Save**.

Note: Before your users will be able to access the Internet, and for IWSS to apply the correct policy, clients will have to run the client registration utility.

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 IWSS and access the Internet. The program file is `register_user_agent_header.exe` located in the installation folder. 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\Internet 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\Internet Settings\User Agent\Post Platform` key called `IWSS:<host_name>/<MAC address>`, where `<host_name>` and `<MAC address>` correspond to the client that ran the utility.

User/Group Name Via Proxy Authorization

IWSS can integrate with the following LDAP servers, and supports both the LDAP 2 and LDAP 3 protocols:

- Microsoft™ Active Directory 2000 and 2003
- Linux™ OpenLDAP Directory 2.2.17
- 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:

	Kerberos	Simple authentication	NTLM
Microsoft Active Directory 2000 and 2003	yes	yes	yes
Linux OpenLDAP 2.2.17	yes	yes	no
Sun Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)	no	yes	no

TABLE 5-1. Authentication methods for supported LDAP servers

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 IWSS send the user's credential (used in the Admin account) as plain text for the initial LDAP connection only.

For increased security protection, IWSS uses the advance authentication method (Kerberos or Digest-MD5) for all subsequent user logon authentications from IWSS to the LDAP server.

Configuring LDAP Settings

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

To configure IWSS to use the user/group name via 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 the **LDAP vendor** that you are using from the list of supported LDAP servers.

   Note: In case future versions of Microsoft Active Directory modify the schema, IWSS 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 choice of LDAP vendor.
6. In the **User Identification** configuration screen, enter the **LDAP server hostname** using its FQDN (Fully Qualify Domain Name).

Note: Entering the LDAP server hostname's IP address is also acceptable, but FQDN format is recommended due to an incompatibility between Kerberos servers and identifying LDAP servers using their IP address.

7. 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 may 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 level of the directory tree you want IWSS 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=us, DC=example, DC=com.

Note: If you're 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* instead of *dc=us,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
- **KDC and Admin Server:** the hostname of the Kerberos key distribution server. If you're using Active Directory, this is typically the same host name as your Active Directory server
- **KDC port number:** Default port = 88

Note: When using NTLM to authenticate with KDC(s) on a different forest through Internet Explorer or using IWSS 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 IWSS 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. 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 IWSS referral chasing configurations are not supported. IWSS uses a different mechanism to query Active Directory servers when the Global Catalog port is enabled, thus configuring referral servers is redundant.

---

12. To verify the information has been entered correctly and IWSS can communicate with the LDAP servers that you configured, click **Test LDAP Connection** on the **User Identification** page. A message box displays, indicating that you have successfully contacted the LDAP server.

13. Click **Save**.

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 will receive those requests on the IWSS server. For more information about enabling the guest account and configuring the guest port, see *Enabling the Guest Port for the Guest Policy* starting on page 8. If the guest port is not enabled, only users in the LDAP directory can browse the Internet.

Enabling the Guest Port for the Guest Policy

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 the client to communicate with IWSS.

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**.

Chapter 6

Configuring HTTP Scanning

This chapter explains the following:

Verifying that HTTP Scanning is Enabled

To verify that HTTP scanning is enabled:

1. Choose **Summary** from the main menu.
2. If the link next to **HTTP Traffic** says **Turn On**, click the link. If it says **Turn Off**, do not click the link.

Creating HTTP 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 HTTP scan policy:

1. Choose **HTTP > Scan Policies** from the main menu.
2. Select **Enable virus scanning** to turn the policy on.
3. Click **Add**.
4. 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.
5. Select the users that this policy will apply to. 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* on page 5-2.

Note: Regardless of the user identification method that you have configured, you can always enter IP addresses of the clients to which the policy will apply.

6. 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.

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 | Use Web Reputation rule in this policy** check box).

2. Ensure that Web Reputation is enabled at the policy level.

   Using the **Add** or **Edit** option for the **HTTP > HTTP Scan > Policies** 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, IWSS 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.

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

IWSS allows you to enable/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.

Specifying the Web Reputation Query Method

The default Web Reputation query method is **DNS and encrypted HTTP**. IWSS 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 **Use DNS and 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**.

   Once 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

IWSS 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 IWSS 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 may need to configure the proxy server to explicitly allow the IWSS IP address to access trendmicro.com.

Negative Results (no match is made; no viruses detected)

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

Positive Results (a match is made showing the presence of a virus)

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, IWSS 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 IWSS 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 6-2)

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 may interrupt IWSS service.

To clear the URL cache:

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

HTTP Virus Scanning Rules

You 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 configure.

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 *Mapping File Types to MIME Content-types* starting on page 1 for how to enter other files types that can be blocked, along with their corresponding MIME content-type.

Specifying File Types to Scan

For more information on IntelliScan and True File Types, see *About IntelliScan* on page 1-20 and *True File Type* on page 1-20.

To select which file types to scan:

IWSS 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**. IWSS 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. Since 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 displays. The default extensions list shows all file types that are known to potentially harbor viruses. This list is

updated with each 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. Click **OK** when you are finished. The screen closes.

Note: 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.

2. You can configure IWSS 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 will not work properly with the resulting delay. You can have IWSS 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 **Block these file types** 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, since it's possible for a MIME content-type to be forged.

Priority for HTTP Scan Configuration

IWSS 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 via the **Add** or **Edit** option for the **HTTP > Scan Policies** screen. IWSS opens and examines the contents of compressed files according to the criteria specified in the HTTP virus scanning configuration screen. IWSS 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).

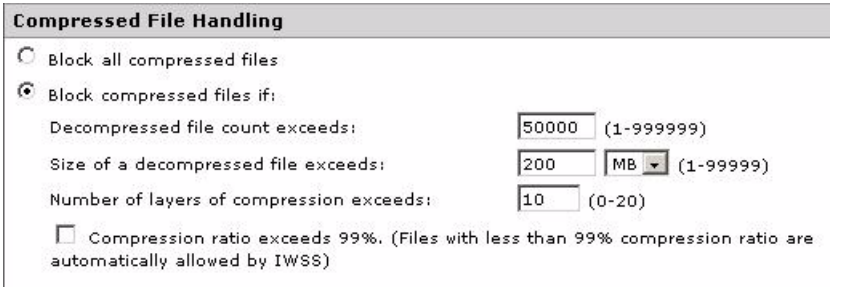


FIGURE 6-1 "Decompression percent" can be used to prevent a denial-of-service (DoS) attack against the IWSS server

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 will not be fulfilled.
- **Block compressed files if...**: Requests to download compressed files that exceed the configured criteria will not be fulfilled. Type values for the following parameters:
  - **Decompressed file count exceeds** (default is 50000)
  - **Size of a decompressed file exceeds** (default is 200MB)
  - **Number of layers of compression exceeds** (0-20, default is 10)
  - **Compression ratio exceeds 99%.** (Files with less than 99% compression ratio are automatically allowed by IWSS).

A compressed file that meets any of the tests will be blocked at the gateway and not scanned.

Handling Large Files

Large file handling can be set via the **Add** or **Edit** option for the **HTTP > Scan Policies** screen.

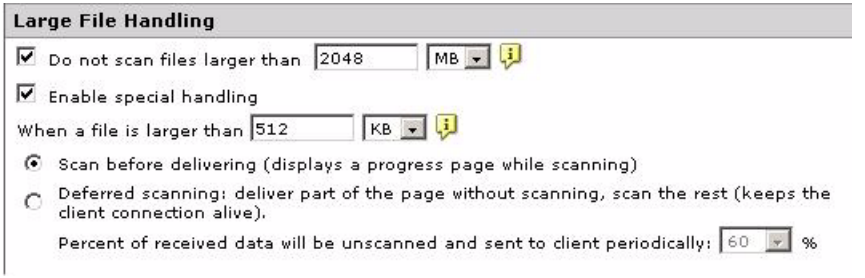


FIGURE 6-2 Handling Large Files

Once you encounter a large file, IWSS scans it in a manner that will reduce the chance of a browser timeout. 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 configure the file size over which files will not be scanned. The default is 2048MB.

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

To use large file handling for HTTP scanning:

1. Under 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 (also see *Scan Before Delivering (Progress Page)* on page 6-11 and *Deferred Scanning* on page 6-11):
   - **Deferred scanning**: loads part of the page while scanning; stops the connection if a virus is found (default setting)
   - **Percent of received data will be unscanned and sent to client periodically:** select a percentage.

Note: Large file handling does not work when using the Blue Coat Port 80 Security Appliance in ICAP mode. If IWSS is configured as an HTTP proxy in-line with the Blue Coat appliance, however, large file handling will function.

3. Click **Save**.

Consider configuring large file handling if your users experience browser timeouts when trying to download files. There are three large file scanning options:

Scan Before Delivering (Progress Page)

When IWSS 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.

Deferred Scanning

When IWSS is configured to use the **Deferred scanning** option, a configurable percentage of a Web page is delivered to the client while IWSS continues to scan the page. If you set the **percent of received data will be unscanned and sent to client periodically** value to 100%, the last 4Kb will not be sent to the client until the scanning is complete.

If you choose to use the deferred scanning option, configure the **percent of received data will be unscanned and sent to client periodically**.

When downloading a large file, 512 bytes of data are released to the requesting client for every 2048KB that is downloaded to the IWSS server.

Important Notes for Large File Handling

- Large file special handling only applies to HTTP scanning, FTP scanning, and FTP over HTTP via the HTTP proxy. It does not apply to FTP over HTTP for ICAP traffic. Users may experience timeout issues while downloading large files using FTP over HTTP.

Violations of the large file handling policy will display a user notification in the requesting client's browser.

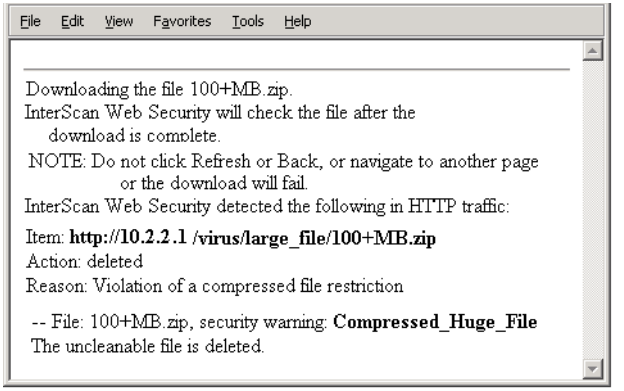


FIGURE 6-3 Notification after completing scanning and downloading the file

Quarantined File Handling

If you choose to quarantine files that IWSS detects as malicious, you can optionally choose to encrypt the files before moving them to the quarantine folder by checking **Encrypt quarantined files**. This will prevent 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

To scan for spyware, grayware and other non-virus additional risks:

1. Under **Scan for Additional Threats** on the **HTTP > Scan Policies > Virus Scan Policy Add/Edit** 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.

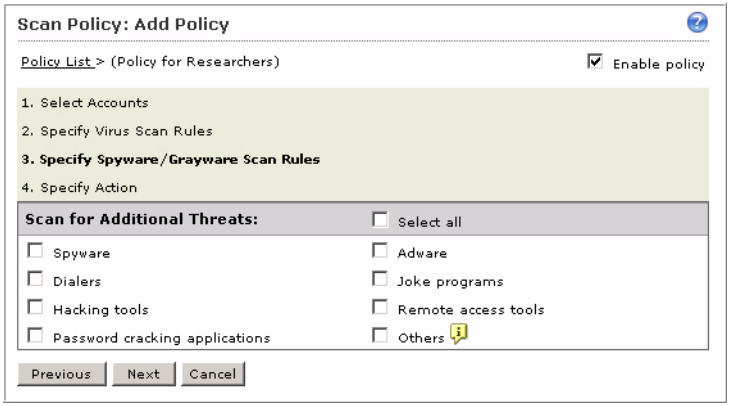


FIGURE 6-4. Spyware, grayware and additional threat scan configuration

Setting the Scan Action for Viruses

After configuring the HTTP virus scanning rules, configure the actions that IWSS will take if an infected file, password-protected or macro-containing file is detected.

Scan Actions

There are four actions that IWSS 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 (by default):

  ```
  {install directory}\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 12.

- Choose **Clean** to have IWSS automatically clean and process infected files. The requesting client will receive 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 pattern file 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 may 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** (recommended and default action) and **Pass**.
- **Macros**: Microsoft Office files that contain macro program code. Since 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 pattern file 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.

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 IWSS.

- 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 will be applied after the database cache expires.

Chapter 7

Configuring Applet/ActiveX Scanning

This chapter explains the following:

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 will apply.

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, IWSS can be configured to either block all applets, or to accept and process applets using the security settings that 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 since it was published. After analyzing the applet's signature, IWSS 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 IWSS that is trusted. The set of these certificates can be viewed and managed by opening the management 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, IWSS 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 IWSS adds monitoring and control code to the applet. Since 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 will execute 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 IWSS 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 will 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 displays. Configure the files and folders where the operation is not allowed.
- To generally 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 IWSS to pass, block or instrument the applet based on its signature and certificate status.
   - Select **Block all Java applets** for IWSS 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 will 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 sub-directories, from the security rule, check **Include files in this and all sub-directories**.

Note: All file paths are those on the client machine, where the applet will run. 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**.
5. Back on the **Java Applet Security Rules** tab, to allow applets to bind to ports on the client workstation, select **Bind local ports**.
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 will 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 will 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**.
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 IWSS 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 will be applied after the database cache expires.

Enter any notes to save pertinent information about this policy, and 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, IWSS 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, IWSS can re-sign applets after instrumentation.

To validate the signature of an ActiveX control, IWSS 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 IWSS 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**.

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 IWSS device's Windows certificate store.

If your environment requires running applets signed with root certificates that are not installed along with IWSS, then add them to the IWSS digital certificate store.

To add a certificate to the IWSS 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

IWSS 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 IWSS 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. IWSS can check whether a certificate has been revoked when a status source is available.

If IWSS cannot access the defined status source, you can configure IWSS to set the status of the certificate to Valid, Unsigned (Strip signature), or Invalid.

Applet Re-signing

IWSS can re-sign instrumented applets with your company's own "private key" before they are sent to client workstations. Since applets lose their original certificates during instrumentation, you may want to re-sign them to ensure that clients' Web browsers will 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 IWSS, 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 will be treated as another unsigned applet—either blocked by the browser or given limited access to system resources.

IWSS 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, IWSS 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 IWSS 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 will be considered valid if it has a valid timestamp countersignature.

If IWSS 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 IWSS 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 IWSS 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 will be "trusted" by IWSS if the root CA certificate of the signature is known to IWSS, is active, and is not flagged.

If IWSS 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 will be collected in this way (signing, intermediate, and root). If required later, a root CA certificate collected this way can be "activated" (made trusted by IWSS) so that the signatures of applets that depend on it can be processed as valid. Intermediate CA and end certificates may be activated, but this will only have 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 may be flagged.

To manage the certificates in the IWSS 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 IWSS 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 will be 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 IWSS.

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 may 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 may be displayed in the client's browser in response to IWSS 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:

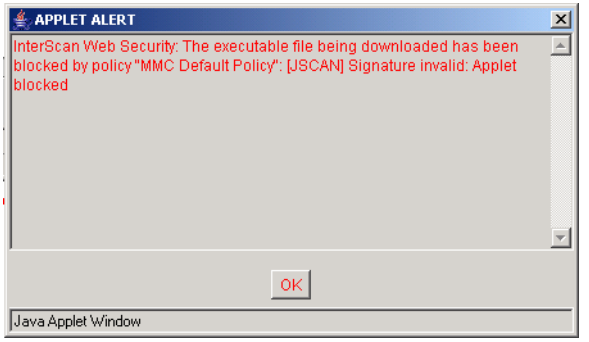


FIGURE 7-1 Blocked applet notification

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 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.

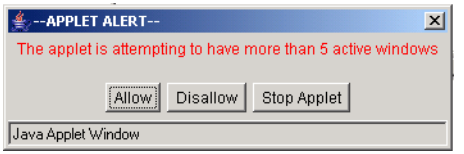


FIGURE 7-2. Applet security violation notification

If the client chooses **Stop Applet**, another notification is displayed to indicate that the applet has terminated.

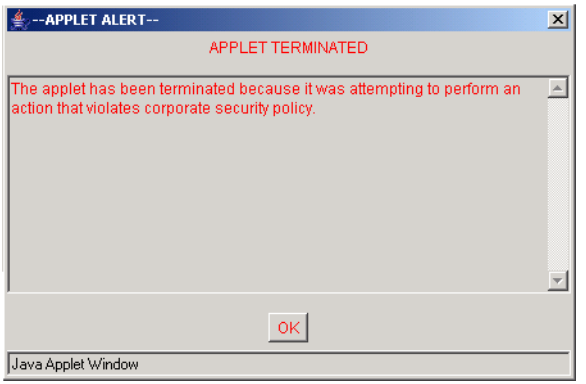


FIGURE 7-3 Applet execution termination notification

Chapter 8

URL Filtering & Intellitunnel Policies

This chapter explains the following:

Managing URL Filtering Policies

IWSS 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 IWSS through the guest port.

Note: The Guest Policy is not supported when IWSS runs in HTTP Forward Proxy mode with LDAP enabled.

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 will apply
- Specify the Web site categories to be blocked during work and leisure time.

To create a new policy:

1. Open the IWSS Web console and click **HTTP > URL Filtering > Policies** from the main menu.

2. Click **Add**.

   The **URL Filtering Policy: Add Policy** screen opens.

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* on page 5-2.

5. Click **Next**.

6. From 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 in the URL Filtering Settings (Schedule tab) page.
   - Select the check box of the category that you want to blocked 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**. Otherwise, the policy will be 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 60 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 Re-classification and URL Lookup

Organized in seven logical groups, IWSS 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 re-classification.

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 **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 may 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 re-classification

To request a URL re-classification:

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 opens.
4. Complete all the necessary information and click **Submit feedback**.

URL Filtering Exceptions

IWSS 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 6-4). 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 `{install directory}\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 `{install directory}\IWSSPIUrlFilter.dsc` file.

To configure the URL filtering approved list:

1. Open the IWSS 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 **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

InterScan Web Security Suite 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.

InterScan Web Security Suite policies permit or block access to URL categories during work and leisure time. By default, InterScan Web Security Suite 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 InterScan Web Security Suite 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 InterScan Web Security Suite 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 which 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 will then be 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.

Creating a New IntelliTunnel Policy

For information on IntelliTunnel, see *IntelliTunnel Notes* on page 4-24.

To create a new IntelliTunnel policy:

1. Select **HTTP** > **IntelliTunnel** from the main menu.
2. Select the **Enabled IntelliTunnel** check box on the top of the screen.
3. On the IntelliTunnel Policies page, click the **Add** link.
4. From the "1. Select Accounts" view of the IntelliTunnel: Add Policy page, specify a policy name.
5. Specify an IP range and/or an IP address and then click **Add**.

   IWSS applies the IM and authentication connections rules to any IP range and IP address you specify. If you are using LDAP, you may see more descriptive information in the Add table, such as the user name.
6. Click **Next**.
7. From the "2. Specify IntelliTunnel Security Rules" view of the IntelliTunnel: **Add Policy** page, select the desired option(s).

   See the IWSS online help for a complete description of the IM and authentication connections protocols.
8. Click **Finish**.

Chapter 9

Access Quotas and URL Access Control

This chapter explains the following:

Managing Access Quota Policies

For information on Access Quota Policies, see *Access Quota Policy Notes* on page 4-26.

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 See *Configuring the User Identification Method* on page 5-2.

   Regardless of the user identification method you have configured, you can always enter IP addresses of the clients to which the policy will apply.
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 will be applied after the database cache expires.

Specifying URL Access Control

IWSS 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 PhishTrap pattern file, a compilation of sites associated with "phishing" schemes or other malicious acts.

For information on Access Quota Policies, see *URL Access Control Notes* on page 4-26.

Configuring Trusted URLs

IWSS can be configured to trust some URLs and exempt them from scanning and filtering. Since this opens a security risk by allowing unchecked content into your network, configuring a URL as "trusted" must be considered carefully. Since 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 IWSS 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 IWSS 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 IWSS will ignore) 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 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*
```

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 will be 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

IWSS 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 IWSS allows requests as usual. Using this feature, you can block a given site yet allow access to some of its sub-sites or files. The URL Blocking list (including exceptions) is maintained in the `\Program Files\Trend Micro\InterScan Web Security Suite\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 PhishTrap pattern file, 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 IWSS 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 will help 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, IWSS will prevent 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, IWSS will consider `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

IWSS 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 IWSS 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 (PhishTrap)

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.

PhishTrap is a Trend Micro service that leverages the following:

- Ability of IWSS 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.

PhishTrap can minimize harm from private and confidential information from being sent out from the client. PhishTrap also prevents access to known phishing URLs.

The URL that is determined to maliciously collect user information will be added to the PhishTrap pattern file. The PhishTrap pattern file is a list of URLs that IWSS will

block. IWSS periodically retrieves the updated PhishTrap pattern file via ActiveUpdate.

IWSS 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 PhishTrap

To block PhishTrap categories:

1. Open the IWSS Web console and click **HTTP > URL Access Control > URL Blocking > Via Pattern File (PhishTrap)**.
2. Make sure that **Enable URL blocking** is enabled.
3. Enable the PhishTrap 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 PhishTrap pattern file.

1. Open the IWSS Web console and click **HTTP > URL Access Control > URL Blocking > Via Pattern File (PhishTrap)**.

2. Type the URL that you want Trend Micro to investigate in the **PhishTrap URL** field.
3. Select the **PhishTrap categories** (either phishing, spyware, virus accomplice, disease vector, or others) that you think the URL is associated with from the menu under **PhishTrap 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 10

FTP Scanning

This chapter explains the following:

Configuring FTP Settings

To configure FTP settings, you need to specify the proxy settings and the data connection.

To configure 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 IWSS 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 or IP address 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; thus one configuration is applied to all clients that access FTP sites through IWSS
- The traffic direction to scan can be configured—either uploads, downloads, or both

Enabling FTP Traffic and FTP Scanning

Before your clients can access FTP sites through IWSS, FTP traffic must be enabled.

To turn on 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 IWSS device is shut down; thus clients cannot connect to any FTP servers through the IWSS FTP proxy. The default setting is **On**.

Once the FTP traffic is enabled, FTP scanning must be turned on.

To enable or disable FTP scanning:

1. Open the IWSS Web console and click **FTP > Scan Rules**.
2. Select **Enable FTP scanning**.
3. Click **Save**.

Priority for FTP Scan Configuration

If the configurations on the **FTP Virus Scan** screen conflict with each other, the program will scan according to the following priority:

1. Block these file types.
2. Scan these file types (if not blocked).

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 A, *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**. IWSS 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 if 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. IWSS 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 pattern file.

  Use this option, for example, to decrease the aggregate number of files IWSS checks, thus decreasing 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 exceeds 99%.** (Files with less than 99% compression ratio are automatically allowed by IWSS).
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 will occur. 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 may result in a virus leak; thus, this would be a performance versus absolute security choice for you. Use this option only if 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 IWSS to take in response to scanning.
13. Click **Save**.

Setting Scan Actions on Viruses

You can specify the action for FTP scanning to take on files:

- Choose **Pass** to send a file to the client without cleaning (Trend Micro does not recommend this choice because it may allow infected files into your network).
- Choose **Quarantine** to move a file to the quarantine directory without cleaning. The requesting client will not receive the file.
- Choose **Delete** to delete a file at the server. The requesting client will not receive the file.
- Choose **Clean** to automatically clean and process a file. The requesting client will receive the cleaned file if it is cleanable.

FTP Access Control Settings

IWSS 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 will not be scanned for a performance benefit.
- The IWSS 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 IWSS (provided FTP traffic is enabled, see *Enabling FTP Traffic and FTP Scanning* on page 10-2).

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 InterScan Web Security Suite. The following are acceptable entries:
   - **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 will identify 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**.

Approved Server IP List

To reduce possible performance issues when accessing trusted FTP sites over which you directly control the content, you can exempt some FTP sites from scanning by adding their IP addresses to an approved list.

Note: Skipping scanning via the IP approved list only applies to file downloads. Uploaded files will still be 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 InterScan Web Security Suite FTP virus scanning.
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 InterScan Web Security Suite FTP server. To increase security, you can selectively allow or deny access to the ports.

To configure IWSS 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 will apply 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 11

Proxy Scan Settings

This chapter explains the following:

Specifying a Proxy Configuration and Related Settings

Choose the scanning mode that corresponds to the physical installation of IWSS on the network.

- **HTTP 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. IWSS and the clients that it protects are typically in the same LAN.
- **ICAP server**—Choose this topology if you have an ICAP client on the network and you want it to pass traffic to IWSS for scanning. IWSS will act as an ICAP server (see *Configuring ICAP Proxy Settings* on page 11-8).

Proxy Configurations

Note: See the *IWSS Installation and Deployment Guide* for details on proxy configurations and planning.

There are several types of proxy configurations:

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

No Upstream Proxy (Stand-alone Mode)

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)

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

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

Note: If IWSS is to be 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 3-2). Certain types of update events utilize the Updates proxy settings to retrieve important information.

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

To configure IWSS 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**.

Simple 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 hostname; configuring policies based on LDAP is not possible.

FTP over HTTP is not available, thus links to ftp:// URLs may not work if your firewall settings do not allow FTP connections. Alternatively, links to ftp:// URLs may work but the files will not be scanned.

Simple transparency is not compatible with some older Web browsers when their HTTP requests do not include information about the host.

HTTP requests for servers that use a port other than the HTTP default port 80 are redirected to IWSS. This means SSL (HTTPS) requests are typically fulfilled but the content is not scannned.

Do not use any source NAT (JIP masquerade) downstream of IWSS, since IWSS needs to know the IP of the client to clean.

A DNS server is needed for DCS to resolve the client computer name from its IP address in order to perform a cleanup.

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**.

WCCP Support

IWSS also supports the Web Cache Coordination Protocol (WCCP 2.0), a protocol defined by Cisco Systems. The same limitations listed for simple transparency also apply to WCCP transparency, with the exception that FTP connections work and downloads via FTP are scanned. The benefits of WCCP transparency are support for multiple routers and automated reconfiguration for load balancing on router(s) when adding or removing IWSS servers.

Trend Micro recommends using Cisco IOS versions:

- 12.2(0) to 12.2(22). Avoid using versions 12.2(23) and above.

- 12.3(10) and above. Avoid using IOS versions from 12.3(0) to 12.3(9).

Note: To use WCCP transparency, you must have a WCCP-compliant router installed on your network. Consult your hardware documentation or the hardware vendor's Web site if you have any questions about hardware compatibility with IWSS. The Cisco PIX firewall does not support WCCP. When using Cisco PIX, transparency can only be enabled using simple transparency.

To configure WCCP support:

1. Select **HTTP** > **Configuration** > **Proxy Scan Settings** from the main menu.
2. Check **Forward proxy**.
3. Check **Enable transparency** and **Use Web Cache Coordination Protocol**.
4. Type the **Router IP address** of your WCCP-compatible hardware.
5. User the **Client Requests** section, change the **Listening port number** to port 80.
6. Click **Save**.

Note: Before configuring IWSS to work with multiple routers, make sure the IWSS is not currently connected to a router. Also make sure the GRE driver is uninstalled before you configure the driver again.

Reverse Proxy

To configure IWSS 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 will protect.
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 will be through SSL, don't forget to configure the HTTPS ports.

To complete your reverse proxy configuration, the IWSS 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 IWSS 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 IWSS Web console and click **HTTP > Configuration > Proxy Scan Settings**.
2. In the **HTTP Listening port** field, type the port number (default values are 1344 for ICAP and 8080 for HTTP Proxy).
3. Click **Save**.

Note: IWSS handles HTTPS connections differently from HTTP connections. Because the data is encrypted, IWSS is not capable of scanning content downloaded via HTTPS. IWSS 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 PhishTrap 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 anonymous FTP logon.

Number of Concurrent Connections

The maximum number of concurrent connections that IWSS will accept is 4000. Beyond this number, IWSS will reject client HTTP requests. At 1200 concurrent connections, the average user will experience approximately two seconds of additional latency while browsing Internet Web pages. Between 1200 and 4000 concurrent connections, latency will increase depending on the complexity of the Web site. By monitoring the concurrent connections displayed on the Summary page, you can monitor how the users' browsing experience may be affected by connection load on the system. You can change the section `[max_concurrent_connections]` in the file `intscan.ini` to configure the concurrent connection settings.

Network Configuration and Load Handling

At 1200 concurrent connections, each IWSS device can process traffic for a community of 3000 users on average. This number assumes that 20% of those users are actively making Internet requests at any one time. To support a larger or more active user community, you will need to configure additional IWSS servers to work together in a server farm.

Enabling the Guest Account (LDAP only)

When using the **User/group name via proxy authorization** identification method, virus scanning, Java applets and ActiveX security, URL filtering, and access quota

policies all support configuring policies for users temporarily visiting your network. These guest policies are applied to clients that connect to IWSS via the "guest" port. The guest account is disabled in the default post-install settings—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 **Enable guest account**.
3. The default **Port number** is 8081 and typically does not have to be modified unless the port is already in use.
4. Click **Save**.

Configuring ICAP Proxy Settings

To configure ICAP proxy settings:

1. On the **HTTP > Configuration > Proxy Scan Settings** screen, choose the **ICAP** option.
2. Choose whether to **Enable "X-Virus-ID" ICAP header** and **Enable "X-Infection-Found" ICAP header**

Chapter 12

Administrative Tasks

This chapter explains the following:

Configuring the Quarantine Directory

During installation, IWSS creates a quarantine directory (default path = `{install directory}\quarantine`) to copy files in response to a security event:

To modify the quarantine directory:

1. Choose **Administration > IWSS Configuration > General** from the main menu.
2. Type the path of the quarantine folder in **Specify quarantine directory** and click **Save**.

Note: Any folder that you specify must exist on the IWSS server. Moreover, map a network drive before configuring the quarantine folder (UNC paths are not supported).

Viewing Database Connection Settings

You can view the database connection settings by clicking **Administration > IWSS Configuration > Database**. To test the connection to the database, click **Test Database Connection**.

Policy settings are stored in the database, and IWSS copies the settings to a memory cache. IWSS reloads the settings from the database into memory according to the time to live (TTL) interval.

To configure the Policy Deployment Settings in minutes:

1. Open the IWSS management console and click **Administration > IWSS Configuration > Database**.
2. Under **Policy Deployment Settings (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 Web Console Password

The Web console password is the primary means to protect your IWSS server 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.

You can use an administrator-level account to change the password of other login accounts. With a report-only account, you can only change your own login account password. An auditor account cannot be used to change any account password.

The following tips will help you design a safe password:

- Include both letters and numbers in your password
- Avoid words found in any dictionary, of any language
- Intentionally mis-spell words
- Use phrases or combine words
- Use both uppercase and lowercase letters

To change the console password:

1. Login into the IWSS console as an administrator user.
2. Open the IWSS console and click **Administration > Login Accounts** in the main menu.
3. Click on an account name in the list.
4. Type your new password in the **Password** field, and then re-type and confirm the new password in the **Confirm Password** field.
5. Type a description.
6. Click **Save**.

Encrypting Browser-console Communication (HTTPS)

To prevent the interception of configuration data when it travels from the management console to the server, IWSS can use secure HTTPS protocol. Tomcat operates only on JKS (Java KeyStore) format keystores, which is Java's standard "Java KeyStore" format, and is the format created by the keytool command-line utility. You can find the executable keytool in the following directory: `[Install_directory]\IWSS\jre\bin` (the default install directory is `C:\Program Files\Trend Micro\InterScan Web Security Suite`).

To create a new keystore that contains a single self-signed certificate:

1. Execute the following from a terminal command line:

   ```
   keytool -genkey -keyalg RSA -alias tomcat-server -keystore
   mykeystore
   ```

2. Follow the on-screen instructions; specify your own unique password when prompted for a password.

   The file mykeystore is generated in the current working directory.

3. From the Administration page, enter the SSL password used to create the mykeystore file.
4. Enter the port number you wish to use for the SSL connection and then save this information.
5. The IWSS Web Console redirects you to the correct port number and then the Login page opens in the Web Console.

   If the IWSS Web Console does not redirect you to the correct port number, then complete the remaining steps.

6. Go to URL https://hostname:port and specify the correct port.
7. Stop and restart the Trend Micro InterScan Web Security Suite Console service.
8. After setting up HTTPS access, rather than using http://<iwss server>:1812, use the following URL (and port) to open the IWSS console:

   https://<iwss server>:8443

9. To enable the certificate, go to the **Services** screen (click **Control Panel** > **Administrative Tools** > **Services**) and manually restart Trend Micro InterScan Web Security Suite for HTTP service.

Accessing the IWSS Console via HTTPS

To encrypt configuration data as it passes from the Web-based console to the server, you must alter the URL to use the HTTPS protocol and specify port 8443 instead of port 1812. Type the URL for encrypted communication (HTTPS) in the following format:

```
https://{SERVER-IP}:8443/index.jsp
https://123.123.123.12:8443/index.jsp
```

Where SERVER-IP is the IP address of the server. For comparison, the URL used for non-encrypted communication (HTTP) is:

```
http://{SERVER-IP}:1812/index.jsp
http://123.123.123.12:1812/index.jsp
```

Disabling Non-HTTPS Access

Once you have enabled HTTPS to encrypt browser-console communication, you can disable non-HTTPS access to avoid the possibility of having your configuration data intercepted.

To disable non-HTTPS access:

1. Edit the Tomcat HTTP configuration file `C:\Program Files\Trend Micro\InterScan Web Security Suite\tomcat\conf\server.xml`.
2. Delete the following nodes:

```
<Connector className=”org.apache.coyote.tomcat4.CoyoteConnecto”

port=”1812”
minProcessors=”5”
maxProcessors=”75”
enableLookups=”true”
redirectPort=”8443”
acceptCount=”100”
debug=”0”
connectionTimeout=”2”000”
useURIValidationHack="false” disableUploadTimeout=”true” />
```

3. Go to the Services screen (click **Control Panel > Administrative Tools > Services**) and manually restart Trend Micro InterScan Web Security Suite Console service.

   After making these changes, the IWSS Web console is accessible only via

   `https://<IWSS_server_IP>:8443/index.jsp`

Configurations After Changing the Console Listening Port

If the management console's listening port is changed, for example, to disable HTTP access, two configuration parameters in the `intscan.ini` file must be modified to continue using a scanning progress page.

Under the [HTTP] section of the `intscan.ini` file, change the following default parameters to reflect the new port and/or protocol:

```
[http]
iscan_web_server=1812
iscan_web_protocol=http
```

For example, if disabling HTTP after enabling HTTPS access to the management console, change the configuration parameters to the following:

```
[http]
iscan_web_server=8443
iscan_web_protocol=https
```

Activating IWSS, URL Filtering, and Java Scanning

You can activate IWSS, URL Filtering and Java Scanning after installation from the IWSS console. To activate IWSS, URL Filtering and Java Scanning, you need to have an Activation Code.

Obtaining an Activation Code

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

Obtaining a Registration Key

The Registration Key can be found on:

- Trend Micro Enterprise Solutions CD
- License Certificate (which you obtained after purchasing the product)

Registering and activating IWSS and URL filtering entitles you to the following benefits:

- Updates to the IWSS pattern file, PhishTrap signature database, and scan engine
- Updates to the URL filtering engine
- Technical support
- Easy access to the license expiration update, registration and license information, and renewal reminders
- Easy renewal of your license and update of your customer profile

---

Note: After registering IWSS, you will receive an Activation Code via email.
An Activation Code has 37 characters (including the hyphens) and is written in the following format: xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
A Registration Key has 22 characters (including the hyphens) and is written in the following format: xx-xxxx-xxxx-xxxx-xxxx

---

When the full version expires, security updates will be disabled. When the evaluation period expires, both the security updates and scanning capabilities will be disabled. In the **Administration > Product License** screen, you can obtain an Activation Code online, view renewal instructions, and verify the status of your product.

To obtain an Activation Code online:

1. Open the IWSS console and click **Administration > Product License**.
2. Click **Enter a new code** and click **register online**. Do one of the following:
   - For new customer registrations, click **Continue** and go to Step 3.
   - For returning customers, enter your Login ID and password, then click **Login** and go to Step 8.
3. The **Enter Registration Key** screen appears. Use the Registration Key that comes with your product (on the Trend Micro Enterprise Solutions CD or License Certificate). Click **Continue**, and then click **I CONFIRM**. in the next screen that appears.

4. The **Confirm Product Information** screen appears. Click **Continue with Registration** to confirm all the product information. Next, type all the required contact information in the fields provided and click **Submit**.
5. The **Confirm Registration Information** screen appears. Click **Edit** to update your contact information and click **OK** to continue.
6. The **Activation Code** screen appears. The system informs you that your Activation Code will be sent to your registered email address.
7. Click **OK**. Go to Step 10.

Note: You are required to change your password the first time you log on.

---

8. The **My Products** screen appears. Click **Add Products** and type the Registration Key. To edit your company profile, click **View/Edit Company Profile**.
9. Your Activation Code appears on the next screen. To receive a copy of your Activation Code through your registered email address, click **Send Now**.
10. Type the Activation Code in the **Activation Code** field and click **Activate**.

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

Managing Login Accounts

Up to 128 users can access IWSS using assigned access rights. When in the application, users can make configuration changes that are recorded in the login accounts log.

About Access Rights

If you have a team of security administrators who are responsible for different functions and who may also have help desk privileges, then assigning them access rights can be beneficial to your organization. To manage IWSS, these users can have different logins with different privileges.

Access rights can also give you the ability to audit what is being changed in IWSS. If you have the need to comply with certain government agency standards, then this function is can be critical.

There are three levels of access:

- Full access—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. This is the default access for new users.
- Auditor—Users cannot make any configuration changes; they can view configurations, logs, and generate real-time reports and view other reports.
- Reports only—Users can only view the Summary pages and scheduled reports. They can generate real-time report queries and change their own password.

Note: With an auditor account, you can generate real-time reports but only view other types of reports.

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 See *About Access Rights* on page 12-9.

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

Audit Log File

The audit log file is where IWSS stores any configuration changes that users make to the application. The log file contains a prefix that you can use to organize your logs.

The log prefix is auto-generated but you can change this in the command line interface (CLI). To change the log prefix, ensure that you have root permission and then from the CLI, open the configuration file `\Program Files\Trend Micro\InterScan Web Security Suite\intscan.ini` and make the necessary changes. Finally, restart IWSS to activate the change.

Configuring an IWSS Server Farm

Multiple IWSS 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 IWSS devices on their network.

Note: An IWSS server farm must have only one primary server.

To configure server designation:

1. Open the IWSS Web console and click **Administration > IWSS Configuration > IWSS Server Farm**.
2. Select **Enable for use in a multiple IWSS 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**.

Registering Control Manager Agent

Before you can use the Control Manager Agent, you have to register it with TMCM.

To register the Control Manager Agent:

1. Go to **Administration > IWSS Configuration > Control Manager Settings** page of the IWSS Web console
2. In the Control Manager Settings page, enter the pertinent information.
3. Click **Register**.

   If the registration is successful, the Connection Manager Status displays: "Registered Control Manager server: Connected" and the **Register** button becomes the **Update Settings** button.

   If the registration is unsuccessful, the Connection Manager Status displays: "Registered Control Manager server: Not connected".

To update MCP Proxy Settings or Two Way Communication Port Forwarding information:

Note: You cannot update the Control Manager Server Settings.

1. Make any necessary changes in the MCP Proxy Settings and/or Two Way Communication Port Forwarding areas.
2. Click **Update Settings**.
3. Wait 20 - 30 seconds to allow the Agent to be updated with the new settings and return you to the Control Manager Settings page.

To update the Control Manager Agent:

1. Unregister the Agent by clicking **Unregister**. Wait 20-30 seconds to allow the Agent to unregister with TMCM.

2. Make the necessary changes and then click **Register**.
3. Wait 20 - 30 seconds to allow the Agent to be updated with the new settings and return you to the Control Manager Settings page.

   The agent is now registered to TMCM with the new Control Manager Server Settings.

Chapter 13

Notifications

This chapter explains the following:

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. IWSS sends administrator notifications via 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. IWSS 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.

Recipient Settings

IWSS sends administrator notifications to email addresses that you specify. The administrator enters email settings when installing IWSS 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** on the top of the screen.
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 IWSS to initial SMTP sessions using the EHLO command.
5. Click **Save**.

Notification Tokens/Parameters

To make notifications more meaningful, InterScan Web Security Suite can use tokens (or variables) as information placeholders in a notification. When an event occurs, InterScan Web Security Suite 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 %d, InterScan Web Security Suite detected a security risk %v
in the file %F. %t attempted to download the file from %U.
```

The notification might read as follows:

```
On 1/23/2007 8:36AM, InterScan Web Security Suite detected a
security risk TROJ_VIPERIK.A in the file game.exe.
123.123.123.12 attempted to download the file from
http://www.example.com.
```

With this information, administrators can contact the client and provide more security information. The notification in this example uses five variables: %d, %v, %F, %t and %U.

The following table contains a list of variables that can be used in notification messages and pages.

TABLE 13-1. Description of variables

Variable	Variable Meaning	How the Variable is Used
HTTP and FTP Scanning		
%Y	Date and time	The date and time of the triggering event

Variable	Variable Meaning	How the Variable is Used
%F	File name	The name of the file in which a risk is detected, for example, anti_virus_test_file.htm
%V	Malware name (virus, Trojan, etc.)	The name of the risk detected
%	The character '%' itself	To insert the percentage character into a notification message or page
%A	Action taken	The action taken by IWSS
%m	Method	The processing method that triggered the event. This variable is not available for use in notifications (email or SNMP).
%M	Moved to location	The quarantine folder location where a file was moved
%H	IWSS host name	The IWSS 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	IWSS host name	
%R	Transfer direction	
%X	Reasons/block type	
%Y	Date and time	
%N	User name	
%V	Virus or Trojan	

Variable	Variable Meaning	How the Variable is Used
Applets and ActiveX Security		
%D	Protocol being scanned	
%H	IWSS host name	
%N	User name	
%U	URL/URI	
%W	New certificate information	used in IWSS's configuration file "IWSSPIJavascan.dsc" by user who need configure its own message of new certificate notification.
%X	Reason	
%Y	Date and time	
%Z	Policy name	
IM and IntelliTunnel Security		
%D	Protocol being scanned (HTTP or FTP)	
%H	IWSS 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	IWSS host name (only works in header field)	
%U	URL/URI (only works in body)	
%X	Reason (only works in body)	
URL Filtering		
%U	URL/URI	
%X	Reason	

Variable	Variable Meaning	How the Variable is Used
Threshold Notification		
%m	Metric	
%t	Threshold value	

Configuring Notifications

To configure a notification, select the types of events that will issue 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, InterScan Web Security Suite only supports uploading HTML files. Any additional files will 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 IWSS detects malicious code in a file requested by a client, it will issue an administrator notification via email and a user notification in the requesting client's browser.

Since 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 3.
4. Type the **Headline** to appear in the browser. The default is *IWSS 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**.

Configure HTTP Blocked File Type Notifications

When IWSS detect end-users trying to access a file which type has been configured to block, it will issue an administrator notification via email and a user notification in the requesting client's browser.

To configure HTTP Blocked File Type notifications:

1. Click **Notifications** and then click **HTTP Blocked File Types**.
2. Under **Administrator Notification**, select **Send a message when ...**.
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* on page 13-3.
4. Type the Headline to appear in the browser. The default is "IWSS Security Event (Server Name)". The header line is common for virus infection messages, file type blocking, and URL blocking messages.
5. Customize messages shown in the browser:
   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 a User Notification Message for Blocked URLs

When IWSS detects an attempt to access a URL in the PhishTrap pattern file or a prohibited URL from the local IWSS list, IWSS 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 IWSS 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 3.
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**.

Configure FTP Blocked File Types Notifications

In addition to scanning FTP uploads and downloads, InterScan Web Security Suite can block file types at the FTP gateway. When the files are blocked, IWSS will issue an administrator notification via email and a user notification at the client's program UI.

To configure FTP Blocked File Type notifications:

1. Click **Notifications** and then click **FTP Blocked File Types**.
2. Under **Administrator Notification**, select **Send a message when ...**.
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* on page 13-3.
4. Customize messages shown in the browser:
   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 independent file.
   c. Verify that the notifications appear correctly by clicking **Preview**.
5. Click **Save**.

Configuring IntelliTunnel Security Notification Settings

When IWSS 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 Notes* on page 4-24.

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 3
4. Click **Save**.

Configuring Applets and ActiveX Security Notification Settings

When IWSS detects an attempt to download a Java Applet or ActiveX object that violates a security policy, the application sends an administrator notification via 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 3.
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

IWSS 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 will trigger 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. IWSS 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

IWSS can send these alerts either through email, SNMP trap/notification (if enabled), or both.

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 3.
4. Click **Save**.

Enabling SNMP Trap Notifications

IWSS 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 > IWSS 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 will trigger 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 IWSS policies, not related to viruses or malicious code
   - **Pattern, database or scan engine updates**—Events related to IWSS updates
   - **IWSS service interruptions**—Issues with any of the essential IWSS services
   - **System performance metric**—IWSS 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 14

Reports and Logs

This chapter explains the following:

Introduction to Reports

IWSS can generate reports about virus and malicious code detections, files blocked, URLs accessed and DCS cleanups. You can use this information about InterScan Web Security Suite program events to help optimize program settings and fine tune your organization's security policies.

You can configure and customize reports. For example, InterScan Web Security Suite 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, IWSS can send notifications via email when a scheduled report is ready for viewing.

Types of Reports

InterScan Web Security Suite 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 InterScan Web Security Suite
- **Individual user reports**

The following is a list of 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 User Reports

- Overview report
- Most popular sites visited 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 may 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 infection

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 IWSS
- **Specific users**: 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 groups**: 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 See *Configuring the User Identification Method* on page 5-2.

Report Type (Consolidated or Individual)

In Scheduled Reports, IWSS can generate consolidated reports, which contain all possible reports. In either Scheduled Reports or Real-time Reports, IWSS can generate individual reports that you specify. For a list of available reports, see *Types of Reports* starting on page 2.

Options

IWSS can present program information in either bar, stacked bar or line charts. Different chart shading for URLs or downloads blocked by IWSS versus successful requests can also be used.

Additional Report Settings

For real-time reports, specify the time period the report will cover.

When setting up a scheduled report, there are some additional settings:

- Send a 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

IWSS 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 will be 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 7.

Note: Groups in the "Specific group(s)" are different from groups in "LDAP group". To have IWSS generate reports for a specific group, you must define a policy for the specific group and that policy is violated. If an event violates more than one policy, a report will only show the violation information for the first matched policy.

5. Under **Report Type**, select the desired report parameter(s).

Note: IWSS 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:

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

Report by	Included Report 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 will be only in "Most blocked URLs."

TABLE 2. Report parameter availability depends on the report type

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**).
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**).
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 InterScan Web Security Suite to generate scheduled reports on a daily, weekly, or monthly basis. To manage the large volume of reports generated, IWSS 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 7 and *To select specific user(s):* starting on page 7.

---

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 IWSS 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 click **Delete**.

Customizing Reports

IWSS 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 IWSS to archive scheduled reports. The default path for archiving reports is `C:\Program Files\Trend Micro\InterScan Web Security Suite\report but can be modified.` but can be modified. The default configuration is to archive 60 daily reports, 20 weekly reports, and 4 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 `{install folder}\report`)

Note: When changing the **Archive Directory**, the folder must exist on the IWSS 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 IWSS: reporting logs and system logs.

Reporting logs provide program event information, and the IWSS 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
- Database import tool
- SNMP service

The database stores all log data. Log data can also be stored in text log files for compatibility with previous IWSS 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

IWSS uses data from reporting logs to generate reports. You can configure InterScan Web Security Suite 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 IWSS user interface. In this case, you can only review the logs by directly opening the generated text files.

Configure reporting log options in the IWSS Web console under **Logs > Settings** (see *Log Settings* on page 14-19 for more information). Text logs provide backward

compatibility with previous versions of IWSS 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 will not be available. Moreover, if IWSS is configured as an upstream proxy, valuable data on user activities may not be available. If you want InterScan Web Security Suite to summarize all Web-related activities, enable the access log under **Logs > Settings > Reporting Logs > Options**.

Note: When the access log is enabled, the InterScan Web Security Suite service is restarted. During the restart, a router may take up to 30 seconds to recognize InterScan Web Security Suite again, during which the router will not redirect packets.

Querying and Viewing Logs

The IWSS 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, once 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.

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 IWSS 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 IWSS, 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:
     - **IWSS-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
     - **PhishTrap defined rule:** Displays a PhishTrap 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 PhishTrap

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. IWSS 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
- IWSS device that processed the access
- IP address of the client system that requested the access

Note: Network address translation may 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 IWSS service is restarted. During the restart, a router may take up to 30 seconds to recognize IWSS again, during which the router will 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 IWSS 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
- IWSS 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 IWSS 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 will be 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 IWSS sends the cleanup request. Since no malware is cleaned during these attempts, querying the cleanup log by malware name will 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, malware 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.
IWSS stores violation logs will in the database. Thus the size of the database may grow exponentially if there is a large amount of violation traffic or access logging is enabled.
Microsoft SQL Server Express 2005 has a database limitation of 4 GB. If the database size exceeds this limit, the SQL Server service will become unstable and multiple event logs with an `MSSQL$IWSS` error will be recorded. If this problem occurs, delete some logs to reduce the size of the database.

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 `{install folder}\log`. A folder must exist on the IWSS device and you must have the correct permission before the folder can be configured as the log file location. IWSS checks after a folder path is entered, and an error message will appear 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 IWSS 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 IWSS to gather performance data and log HTTP/FTP access events. If you enable these, configure the logging interval.

The default time period that logs will be 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 will be updated with new logs (default = 30 seconds).

Log File Naming Conventions

By default, log files are written to the `{install folder}\log` directory. IWSS has a standard convention for naming log files. For instance, the convention for virus logs is:

```
virus.log.2007.01.09
```

which can be read as virus log for January 9, 2007

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

TABLE 3. 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

TABLE 3. Log files naming conventions

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
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
SNMP Service Log	snmp_monitor.log.yyyymmdd.0001

Note: Deleting a log will not necessarily prevent the corresponding data from appearing in the IWSS Web console. To prevent InterScan Web Security Suite from displaying data, you must remove the corresponding data from the appropriate database table.

TABLE 4. Major database tables for IWSS logging/reporting

Table Name	Example Columns
tb_url_usage	username, url, path
tb_report_by	period, category, entity_type, entity_name

TABLE 4. Major database tables for IWSS logging/reporting

Table Name	Example Columns
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, IWSS 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 IWSS device.

The character format that IWSS 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.

Appendix A

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 will be blocked

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

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/ wordper-fect	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-strea m
exec	application/ x-msdown-load	exe	application/ octet-stream	fh9	image/ x-freehand

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
fli	video/x-fli	fm	application/vnd.frame-maker	gif	image/gif
gzip	applica-tion/x-gzip	gzip	encoding/x-gzip	hpexe	application/octet-stream
iff	audio/x-aiff	java	text/x-java-source	java	application/java-class
java	applica-tion/x-java-applet	java	applica-tion/x-java-vm	java	text/x-java-source
java	application/java-class	java	applica-tion/x-java-applet	java	applica-tion/x-java-vm
jpeg	image/jpeg	jpeg	image/pjpeg	lha	application/x-lha
lisp	application/x-lisp	maud	audio/x-maud	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
msdoc	application/msword	msexl	application/excel	msexl	application/x-msexcel

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
msexl	application/x-excel	msexl	application/vnd.ms-excel	msmdb	application/x-msaccess
msppt	application/mspowerpoint	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
ras	image/x-cmu-raster	ras	image/cmu-raster	risc	application/octet-stream

File type	MIME content-type	File type	MIME content-type	File type	MIME content-type
rmf	application/ vnd.rn-real media, g_audiovid eo	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-uuen-code	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 B

Configuration Files

There are three types of configuration files (main, protocol module, scanning module). All the configuration files are in the `{IWSS root}` directory; the default location for `{IWSS root}` is `\Program Files\Trend Micro\InterScan Web Security Suite\`. 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}\urlfcIFX.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 IWSS server are in:

`{IWSS root}\ClientACL_http.ini and {IWSS root}\ClientACL_ftp.ini`

- Settings for rules that define what ports IWSS will forward HTTP and FTP requests to are in:

```
{IWSS root}\HttpPortPermission_http.ini and {IWSS
root}\HttpPortPermission_ftp.ini
```

- Settings for rules that define what ports IWSS will allow HTTPS tunneling to are in:

`{IWSS root}\HttpsConnectACL_http.ini`

- Settings for list of IP address and IP ranges of trusted servers are in:

```
{IWSS root}\ServerIPWhiteList_http.ini and
{IWSS root}\ServerIPWhiteList_ftp.ini
```

If you have been using a previous version of IWSS, there are also many new features available in IWSS 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. IWSS provides a choice of either an ICAP protocol handler, which enables IWSS to act as an ICAP server, or an HTTP proxy handler, wherein IWSS acts like a direct HTTP proxy server. 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 IWSS provides content scanning using the scan engine.

Each scanning module has a configuration file with a `.dsc` extension. The IWSS application locates the available scanning modules by searching for `.dsc` files in the directory that is provided in the entry `plugin_dir` under the section `[scan]` in the `intscan.ini` file.

Appendix C

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 IWSS 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 ProductShortNameVariable 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 IWSS 3.1:

- cyrus-sasl-2.1.19
- db-4.2.52.NC
- heimdal-0.6.2
- openldap-2.2.17
- openssl-0.9.7d

Configuration Files

Using OpenLDAP with IWSS 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 since IWSS 2.5 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 IWSS 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.

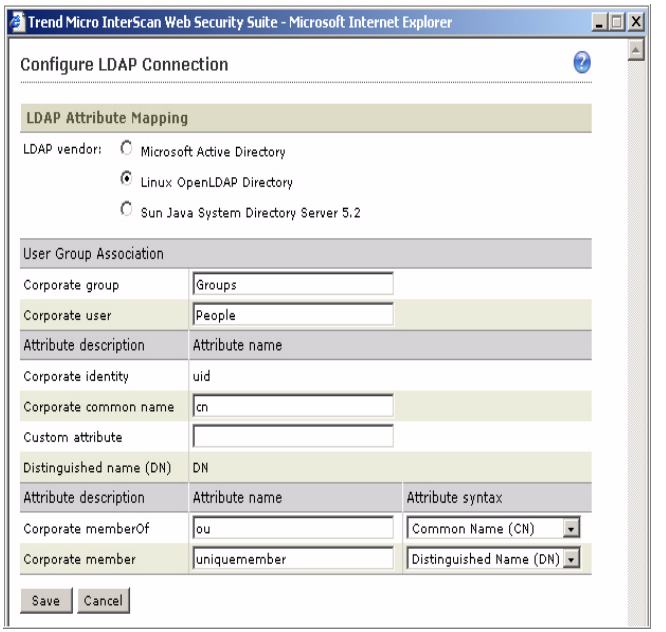


FIGURE 1. OpenLDAP attribute mapping configuration screen

The "Corporate group" field tells IWSS 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. Since LDAP cannot distinguish whether an entry is group or user-specific, IWSS 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 since 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 IWSS needs to associate and look up to locate the group or member entry in the LDAP server. IWSS 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=petery,ou=People,dc=client,dc=us,dc=trendnet,dc=org
givenName: Peter
telephoneNumber: +1 408 555 5555
sn: Peter
ou: All of IWSS Developer Team
ou: People#Corporate User field
mail: petery@peter.com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: petery
cn: Peter Yen

dn: cn=All of IWSS Developer
```

Team,ou=Engineering,ou=Groups,dc=client,dc=us,dc=trendnet,dc=org
ou: Groups #Corporate Group field
ou: Engineering
description: All of IWSS Developer Team
objectClass: top
objectClass: groupOfUniqueNames
uniqueMember:uid=petery,ou=People,dc=client,dc=us,dc=trendnet,dc=org
cn: All of IWSS Developer Team

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:

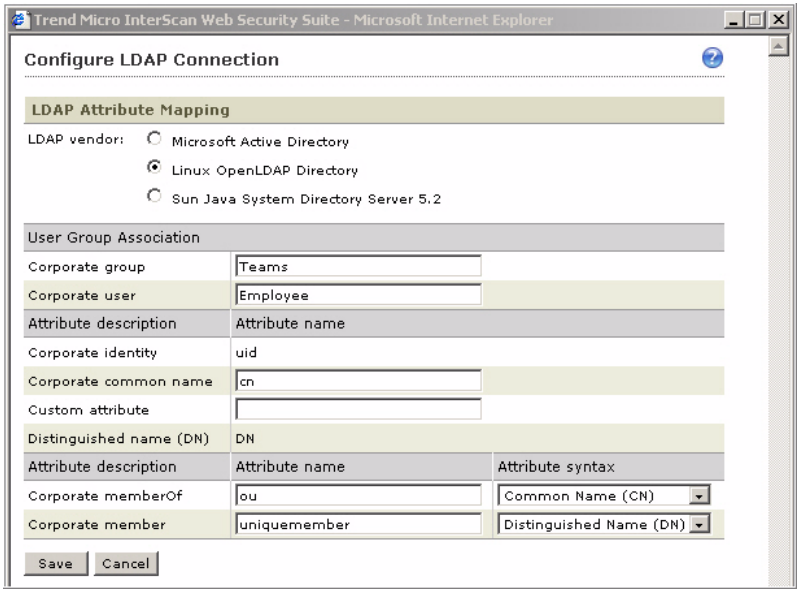


FIGURE 2. OpenLDAP attribute mapping configuration screen

```
dn: uid=petery,ou=People,dc=client,dc=us,dc=trendnet,dc=org
givenName: Peter
telephoneNumber: +1 408 555 5555
sn: Peter
ou: All of IWSS Developer Team
ou: Employee#Corporate User field
mail: petery@peter.com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: petery
cn: Peter Yen

dn: cn=All of IWSS Developer
Team,ou=Engineering,ou=Groups,dc=client,dc=us,dc=trendnet,dc=org
ou: Teams #Corporate Group field
ou: Engineering
description: All of IWSS Developer Team
objectClass: top
objectClass: groupOfUniqueNames
teamMember: Peter Yen
cn: All of IWSS Developer Team
```

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.

Index

G

H

I

T

U

V

W