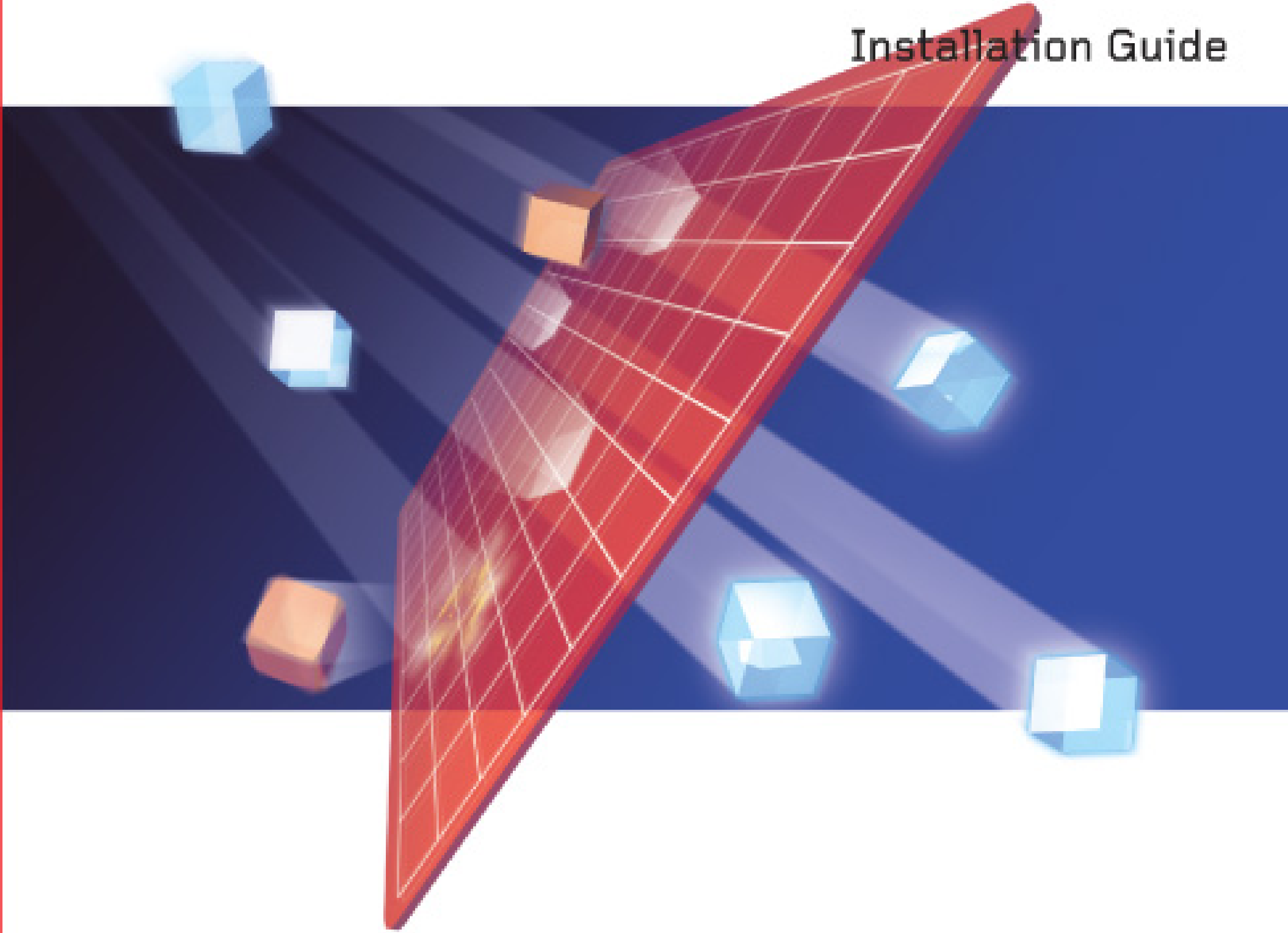
TREND MICRO™

InterScan™ Web Security Suite 3

Antivirus and Content Security at the Web Gateway

for LINUX™

Installation Guide



TREND MICRO™

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

http://www.trendmicro.com/download

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

Document Part No. IHEM32860/60920

Release Date: February 2007

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

The Installation Guide for Trend Micro™ InterScan™ Web Security Suite is intended to introduce the main features of the software and installation instructions for your production environment. 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 technical support information and contact details. Detailed information about how to use specific features within the software is available in the online help file and the 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

PLANNING / PRE-INSTALL CHECKLIST

DEPLOYMENT CHECKLIST

INSTALLATION CHECKLIST

MIGRATION CHECKLIST

CONFIGURE CHECKLIST

Appendix A: Deployment Planning and Staging

Appendix B: Deployment Integration

Appendix C: Tuning and Troubleshooting

Appendix D: Additional IWSS Testing

Appendix E: Advanced Deployment Functions

Appendix F: Protecting a Dedicated Server

Appendix G: Maintenance and Technical Support

Index

Preface

Welcome to the *Trend Micro™ InterScan Web Security Suite 3.0 Installation Guide*. This guide helps you to get "up and running" by introducing InterScan Web Security Suite (IWSS), assisting with deployment, installation, migration (if necessary), initial configuration, troubleshooting, performance tuning, and main post-installation configuration tasks. It also includes instructions on testing your installation using a harmless test virus, troubleshooting, and accessing Support.

This preface discusses the following topics:

- *Audience* on page ix
- *Using the IWSS Installation Guide* on page x
- *InterScan Web Security Suite Documentation* on page xi
- *Document Conventions* on page xii

Audience

The IWSS documentation is written for system administrators in medium and large enterprises. The documentation assumes that the reader has in-depth knowledge of networks schemas, including details related to the following:

- HTTP and FTP protocols
- Database configuration

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

Using the IWSS Installation Guide

The beginning of a section is indicated by a checklist page. The tasks listed on the checklist references related sections in the manual. You can print the checklist and check off each task as you complete them. The gray text indicates that a task is not required and may be an advanced operation.

This guide is divided into the following sections:

Section	Tasks
1 Planning / Pre-install	☑ Verify System Requirements ☑ Know the Information Needed to Install ☑ Acquire Registration Keys and Activation Codes
2 Deployment	☑ Identify Your Operating Mode ☑ Identify Your Server Placement ☑ Plan Network Traffic Protection ☑ Determine HTTP Packet Flow ☑ Determine FTP Packet Flow ☑ Review connections and properties dependencies ☑ Integrate with LDAP ☑ Integrate with Damage Cleanup Services (DCS) ☑ Integrate with Cisco router ☑ Hardening your OS
3 Install	☑ Install IWSS ☑ Change password to confirm successful installation ☑ Enter your activation code
4 Migration	☑ Back up the previous version of IWSS ☑ Back up the Database ☑ Install the latest version of IWSS ☑ Change password to confirm successful installation

5 Configure	☑ Hardware or Non-policy Setup ☑ Set up HTTP Policies ☑ Set up FTP Policies ☑ Perform LDAP Turning ☑ Testing IWSS

InterScan Web Security Suite Documentation

In addition to the *Trend Micro™ InterScan Web Security Suite 3.0 Installation Guide*, the documentation set includes the following:

- **Administrator's Guide**—this guide provides detailed information about all InterScan Web Security Suite 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, and using logs and reports.
- **Readme file**—the Readme 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/`
- **Online help**—Helps you configure all features through the user interface. You can access the online help by opening the Web console and then clicking the help icon (?).

  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 InterScan Web Security Suite management console.
- **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://esupport.trendmicro.com/support`

The Administrator's Guide and readme are available on the InterScan Web Security Suite CD and at http://www.trendmicro.com/download.

Document Conventions

To help you locate and interpret information easily, the InterScan Web Security Suite 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

Section 1

Planning / Pre-install Checklist

☑	Step	**Optional**	**Reference**
	Verify System Requirements		
	Verify host operating system		page 1-1
	Verify hardware		page 1-1
	Verify further requirements	■	page 1-3
	Verify client requirements		page 1-1
	Evaluate or purchase IWSS (acquire a registration key and activation code)		page 1-5
	Know the Information Needed to Install		
	Type of HTTP handler		page 1-3
	Type of proxy configuration		page 1-3
	Control Manager server information	■	page 1-4
	Database type and location	■	page 1-4
	Notification email settings		page 1-3
	SNMP notifications	■	page 1-4
	Proxy for Internet updates	■	page 1-5
	Fresh install or migration		page 1-5
	Remote or local installation		page 1-5
	Acquire Registration Keys and Activation Codes		

☑	Step	**Optional**	**Reference**
	For the following: • Main Program • HTTP Scanning • FTP Scanning • SNMP Notifications IWSS Registration Key: ______________________________ IWSS Activation Code: ______________________________		page 1-5
	URL Filtering (separate access code) IWSS Registration Key: ______________________________ IWSS Activation Code: ______________________________	■	page 1-5
	Applet and ActiveX scanning (separate AC) IWSS Registration Key: ______________________________ IWSS Activation Code: ______________________________	■	page 1-5
	Control Manager agent (separate access code) IWSS Registration Key: ______________________________ IWSS Activation Code: ______________________________	■	page 1-5
	ICAP license # (if used) ______________________________	■	page 1-5

☑	Step	Optional	Reference
	Control Manger (DMS) (separate access code) IWSS Registration Key: ______________________________ IWSS Activation Code: ______________________________	■	page 1-5

Chapter 1

Pre-installation Planning

This chapter guides you through the information gathering phase of deploying IWSS. It describes:

Server Requirements

Operating System

Red Hat Linux

- AS 3.0
- EL 4.0 AS
- EL 4.0 ES

Novell SuSE Linux

- Enterprise 10 Edition

Hardware Requirements

- 2.4 GHz Intel™ Pentium™ 4 processor or equivalent
- RAM:
  - 1GB RAM

    - 3GB RAM recommended with URL filtering installed
    - An extra 128MB RAM with Applets and ActiveX security installed
- Disk space:
    - 2GB disk space for program files with URL filtering installed
    - 150MB disk space for program files without URL filtering
    - Swap partition that is four times the amount of physical memory
    - 125MB disk space to install PostgreSQL
- Monitor that supports 800 x 600 resolution at 256 colors or higher
- Microsoft™ Internet Explorer 6.0 or Mozilla Firefox 1.5 to access the IWSS Web console

Other Possible Requirements

- Database requirements:
    - PostgreSQL v7.4.8 (included)
    - When using multiple IWSS Servers in a server farm configuration, Trend Micro recommends that you use separate server (possibly clustered) for PostgreSQL
    - 1.7GB of disk space for every 3 million HTTP requests per day in order to maintain log files (calculation based on access logging enabled)
    - 256MB of RAM (based on access logging enabled, else 64MB)
- For Internet Content Adaptation Protocol (ICAP), IWSS supports the following:
    - NetApp™ NetCache™ release 6.0.1
    - Blue Coat Systems™ SGOS v4 (latest version)
    - Cisco ICAP servers: CE version 5.3
    - Any cache server that is ICAP 1.0 compliant
- Directory Servers:

  To configure policies based on Lightweight Directory Access Protocol (LDAP) users and groups, IWSS can integrate with the following LDAP directories:
    - Microsoft Active Directory 2000 and 2003
    - Linux OpenLDAP Directory 2.2.16

- Sun™ Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)

Further Requirements

- Administrator or Domain Administrator access to the server machine
- IWSS clients must be able to access the HTTP port of the IWSS server that is selected during the install
- IWSS server must be able to communicate via the client communication port selected during the install to all IWSS clients
- IWSS server and IWSS clients must be able to perform ICMP echo / reply sequences - either using the DNS name or IP address depending on the server selected during the install

Information Needed to Install IWSS

You can either purchase IWSS or download a 30-day trial version of IWSS. The 30-day trial versions provides all the functionality of IWSS.

The IWSS setup program prompts you for required information, depending on the options chosen during installation:

Type of HTTP Handler

If installing HTTP scanning, you will be prompted to choose the type of HTTP handler to install. Installing IWSS as a stand-alone proxy allows IWSS to act as the network's proxy server or work in conjunction with another proxy. Alternatively, you can install IWSS to act as an ICAP server. For more information, See *Planning HTTP and FTP Service Flows* on page A-14.

Type of Proxy Configuration

The most common proxy configuration is to install IWSS as a forward proxy to protect clients from risks they might download from the Internet. Clients will have to modify their Internet connection settings to use the IWSS server as its proxy, unless you enable transparency. However, enabling transparency limits the user identification method to IP address and/or hostname and may make some FTP links inaccessible.

Another installation scenario is to configure IWSS as a reverse proxy, to protect a Web server from having malicious content uploaded to it. For more information, see *Planning the HTTP Flow* on page A-14 and *Planning FTP Flows* on page A-28.

Control Manager Server Information

If you plan to register IWSS with an existing Control Manager server on the network, you need to know the server's host name or IP address and its logon name. Do not install IWSS on a TMCM server.

Database Type and Location

IWSS uses the PostgreSQL database for report logs, policies, rules and configuration settings. Install an instance of PostgreSQL unless you already have an existing instance.

IWSS sends notifications in response to many security risk detections, policy violations or program events. The setup program prompts for the email address to send notifications, and an SMTP server that allows message relay from the IWSS server.

SNMP Notifications

If you plan to use SNMP notifications, the IWSS setup program installs the SNMP agent.

The setup program will prompt for several other SNMP settings including the community name, host name, object identifier (OID), location and a contact name. It will also prompt you for the host, community name, port number and default trap community of the host that can receive SNMP traps.

Management Console Password

Access to the IWSS management console is controlled through a password that is set during installation.

Proxy for Internet Updates

If you have a proxy between IWSS and the Internet, enter the proxy’s host name or IP address, port and an account.

Activation Codes

Activating the three IWSS modules (core program, URL Filtering, and Applet and ActiveX Scanning) requires three separate activation codes. IWSS usually comes with registration keys for the modules purchased. During product registration, the Registration Keys are exchanged for Activation Codes that “unlock” the program. You can register the installation and exchange registration keys for activation codes from a link in the setup program. Alternatively, you can register and obtain activation codes before installing by visiting Trend Micro’s online registration Web site at:

`http://olr.trendmicro.com.`

Fresh Install or Migration

To install IWSS as a fresh install or to migrate from IWSS 2.x to the current version of IWSS, run the `./install_iwss.sh` script. See Chapter 3, *Installing InterScan Web Security Suite* or Chapter 4, *Migrating to InterScan Web Security Suite*.

Remote or Local Installation

IWSS can be installed to either a local or remote server. To remotely install on a UNIX system, you need to connect to that system via NFS, and from that system's console execute the IWSS installer.

Section 2

Deployment Checklist

☑	Step	**Optional**	**Reference**
	Identify Your Operating Mode		
	Select the appropriate mode:		
	• Process mode		page 2-1
	• Thread mode		page 2-2
	Identify Your Server Placement		
	Select the appropriate placement:		
	• Two firewalls with DMZ		page 2-3
	• One firewall with no DMZ		page 2-4
	Plan Network Traffic Protection		
	Re-configuring client settings	■	page A-10
	Using a Layer-4 switch	■	page A-11
	Using an ICAP-enabled proxy	■	page A-12
	Determine HTTP Packet Flow		
	Select the appropriate flow:		
	• HTTP Proxy in Standalone Mode	■	page A-15
	• Standalone mode with multiple servers	■	page A-17
	• HTTP proxy in Dependent Mode (proxy ahead)	■	page A-17
	• HTTP proxy in Dependent Mode (proxy behind)	■	page A-19
	• HTTP double proxy in Dependent Mode	■	page A-20
	• HTTP proxy in Transparent Mode	■	page A-22

☑	Step	Optional	Reference
	• HTTP reverse proxy in Dependent Mode	■	page A-23
	• HTTP proxy in ICAP mode	■	page A-24
	Determine FTP Packet Flow		
	Select the appropriate packet flow:		
	• FTP proxy in Standalone Mode	■	page A-28
	• FTP proxy in Dependent Mode	■	page A-29
	Review connections and properties dependencies		
	Connections and properties	■	page E-1
	Integrate with LDAP		
	Support multiple LDAP servers	■	page B-3
	Global catalog	■	page B-3
	Guest accounts	■	page B-4
	Integrate with Damage Cleanup Services (DCS)		
	Damage Cleanup integration	■	page B-5
	Integrate with Cisco router		
	Integrate with Cisco router (policy 1)	■	page B-7
	Integrate with Cisco router (policy 2)	■	page B-7
	Hardening your OS		
	Pre-OS installation procedures for hardening	■	page E-2
	OS installation procedures for hardening	■	page E-3
	Post-OS installation procedures for hardening	■	page E-4
	Review the top ten UNIX security vulnerabilities	■	page E-4

Chapter 2

Deployment

Identifying Your Operating Mode

InterScan Web Security Suite supports both Process and Thread modes for either ICAP or standalone.

Process Mode

Process mode is the standard operating mode for an HTTP Proxy. Thread mode is more commonly used with ICAP implementations.

Process mode runs the daemon in a multi-process/single thread model, where a parent process has many child processes. The parent process manages all of the child processes. Each child process handles one connection.

TABLE 2-1. Process Mode

Advantages	Limitations
It provides more reliability. Each connection is isolated from other connections as well as from the parent, so in the event of a program fault, only a single connection is affected.	Each connection requires a child process, and each process has a significant memory footprint which can limit the maximum number of child process that can be spawned, and therefore limit the maximum number of concurrent connections.

Advantages	Limitations
There is very little communication overhead because each child process has little communication with either its parent or other child process. This translates to greater throughput, in cases where network latency is low.	

Thread mode

Thread mode runs the daemon in a single-process/multi-thread model. Connections are handled by the worker threads and not by the process. The number of worker threads remains constant until you modify it, and each thread can handle many simultaneous connections.

Note: For optimal performance, Trend Micro recommends a setting of three threads per CPU.

TABLE 2-2. Thread Mode

Advantages	Limitations
The daemon has a small footprint, typically between 200 to 500MB of virtual memory, even with hundreds of connections open. The CPU, not the number of worker threads or memory, limits the number of connections that the threaded daemon can handle.	All the threads occupy the same process space; therefore, if a programming fault causes one thread to crash it will stop the daemon.
Idle connections do not tie up worker threads. In cases where network latency is high, the threaded daemon can continue servicing new and active connections long after the process mode daemon has rejected new connections due to the lack of free child processes.	Some computations require more overhead than in process mode, due to the need to synchronize access to shared memory. This can result in lower throughput when network latency is low.

Identifying Your Server Placement

The first step is to identify the existing server where IWSS server should be installed. The second step is to identify the deployment options that exist, and eliminate those that do not fit the requirement.

Today's enterprise network topologies typically fall into one of two categories:

- Two firewalls with a Demilitarized Zone (DMZ)
- One firewall without a DMZ.

The ideal location for the IWSS server depends upon the topology in use.

Two Firewalls with DMZ

Given today's security concerns, many organizations have implemented a topology consisting of two firewalls (one external and one internal). These firewalls divide the network into two main areas:

- **The DMZ**—The DMZ is located between the external and internal firewalls. Hosts that reside in this area can accept connections from servers that are external to the organization's network. The configuration of the external firewall lets packets from external computers only reach servers inside the DMZ.
- **Corporate LAN**—These segments are located behind the internal firewall. The configuration of the internal firewall passes traffic to machines on the corporate LAN only when the traffic originates from computers inside the DMZ.

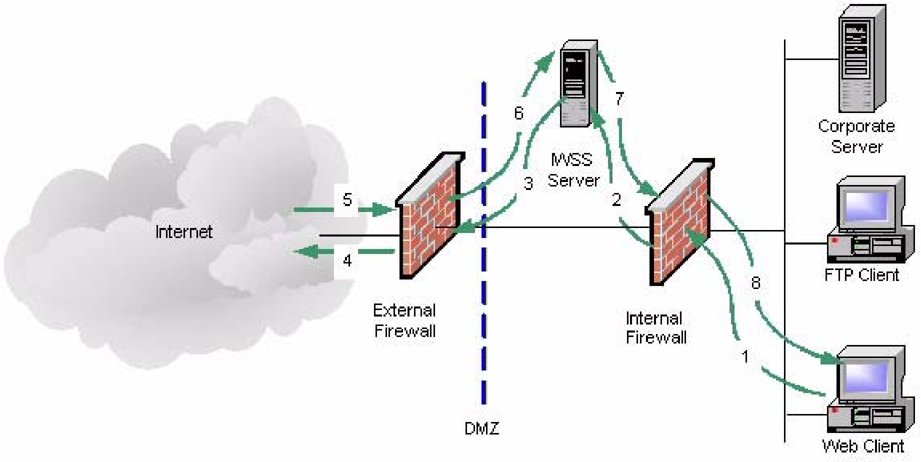


FIGURE 2-1 Two Firewalls with DMZ

This topology requires that all data inbound from the external servers (such as those on the Internet) first pass through a server in the DMZ. It also requires that certain types of data (for example HTTP and FTP packets), outbound from internal segments, pass through a server in the DMZ. This forces the use of proxies such as IWSS.

One Firewall with No DMZ

Some organizations have a firewall, but no DMZ. When using the "no DMZ" topology place the IWSS server behind the firewall.

- Because the IWSS server is not isolated from the corporate LAN, there is one less hop between external machines and machines on the corporate LAN. As shown in the diagram, this results in two less steps for processing a request, one outbound and one inbound.
- The firewall configuration allows connections to machines on the corporate LAN. For security, the firewall must limit the types of data that can reach machines on the LAN. For example, the firewall might allow HTTP data from the Internet to reach only the IWSS server.

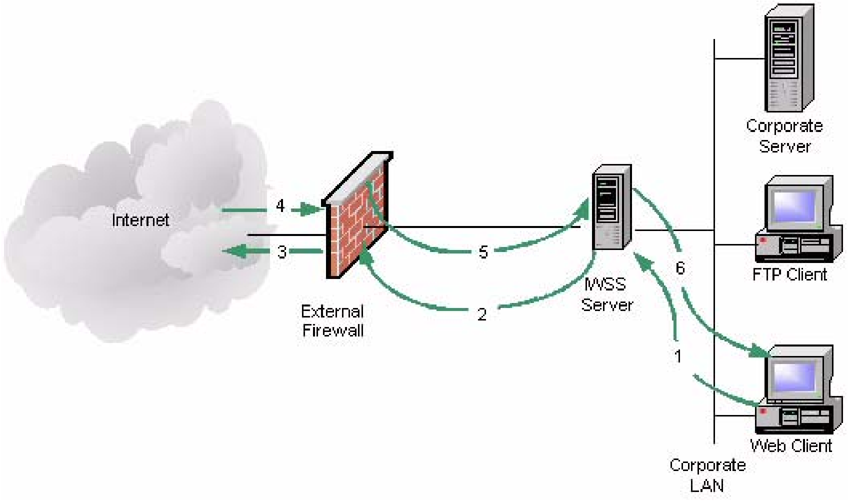


FIGURE 2-2 One Firewall with DMZ

Planning Network Traffic Protection and HTTP and FTP Service Flows

Network Traffic

To enforce the network traffic protection using IWSS, an additional solution (hardware, software or configuration) must be introduced that redirects the HTTP and/or FTP traffic to IWSS. Those solution include the following:

- Reconfiguring client settings
- Using a Layer 4 switch
- Using an ICAP-enabled proxy

See Appendix A, *Deployment Planning and Staging* starting on page A-1 for complete details.

HTTP and FTP Service Flows

Each HTTP and FTP configuration has implications for configuring IWSS, configuring the network, and for network security.

Create a flow plan for the HTTP and FTP services by doing the following:

- Understand each IWSS services purpose and function
- Determine each service's valid data sources. For example, does the HTTP service receive requests directly from the HTTP browsers, or indirectly through an ICAP proxy device?
- Determine which ports to use for the service. For instance, by default, the HTTP service uses port 8080, and the FTP service uses port 21. However, if another application or service is using port 8080, the administrator must configure the HTTP service to use a different port.
- Determine each services valid data destinations. For example, does the HTTP service send validated requests directly to the Web site? Or, does the HTTP service send the validated request to an upstream HTTP proxy?
- Add in any service-specific considerations. For instance, the HTTP service flow might include an ICAP device, but the FTP service flow does not.

Using the information gathered above, administrators determine which one of the possible flows to use for the installation.

See Appendix A, *Deployment Planning and Staging* starting on page A-1 for complete details.

Section 3

Installation Checklist

☑	Step	**Optional**	**Reference**
	Install IWSS		page 3-2
	Open the IWSS Web console		page 3-4
	Change admin password		page 3-6

Chapter 3

Installing InterScan Web Security Suite

This chapter describes the InterScan Web Security Suite components that are part of the installation and how to install and validate an installation.

Component Installation

Note: Trend Micro recommends installing InterScan Web Security Suite on a dedicated server.

During installation, the following components are automatically installed:

- **Main Program**—Management console and the basic library files necessary for IWSS.
- **HTTP Scanning**—Service necessary for HTTP scanning (either ICAP or HTTP proxy) and URL blocking.
- **FTP Scanning**—Service necessary for FTP scanning.
- **URL Filtering**—Service necessary for URL filtering (not enabled by default). Requires a separate activation code.

- **Applets and ActiveX Scanning**—Service necessary for scanning Java applets and ActiveX controls. Requires a separate Activation Code.
- **IntelliTunnel Security**—Services to block communication provided by certain Instant Message (IM) protocols and certain authentication connection protocols.
- **SNMP Notifications**—Service to send SNMP traps to SNMP-compliant network management software.
- **Control Manager Agent for IWSS**—Files necessary for the Control Manager agent. You need to install the agent if you are using Control Manager (Trend Micro's central management console).

Note: URL Filtering and Applets and ActiveX Scanning each require a separate activation code.

Installing InterScan Web Security Suite

Trend Micro recommends that you install InterScan Web Security Suite on a dedicated server. To install InterScan Web Security Suite, you must log on to the target server as **root**.

You can install InterScan Web Security Suite from the Trend Micro Enterprise Solutions CD or download the installation files from the Web.

Note: An activation code is required to enable scanning and product updates (see *Activating IWSS and URL Filtering* on page 5-39).

To install from the Trend Micro Enterprise Solutions CD:

1. Insert the CD-ROM disc into the CD-ROM drive of the server where you want to install IWSS.
2. Choose **InterScan Web Security Suite** from the **Choose a product** drop-down menu and then click **Go**.
3. Run the install script from the product folder on the Enterprise Solutions CD.

To download an evaluation version:

1. Go to the Trend Micro Web page:

   `www.trendmicro.com`.
2. From the **Product & Services** tab, select **Enterprise** from the drop-down list.
3. From the **Complete Product List** drop-down list, select **InterScan Web Security Suite**.
4. From the **InterScan Web Security Suite** page, click the **Download Evaluation Copy** link.
5. From the **Download InterScan Web Security Suite** page, complete all the required fields, accept the license agreement, and then click **Submit Form**.

   A page opens thanking you for downloading an evaluation version of InterScan Web Security Suite. This page states that you will receive an email from Trend Micro containing the links necessary to download the 30-day free trial versions of IWSS.
6. Download the InterScan Web Security Suite product to a temporary directory on the server where you want IWSS to run, and then extract the files.

To download and run the IWSS 3.0 script:

1. Download the installation tar package from the Trend Micro Update Center.
2. Extract the installer components by running the following:

   ```
   tar xvzf iwss_30_linux_b1218.tgz
   ```
3. From the directory containing the InterScan Web Security Suite installation files, type `./install_iwss.sh` and then press **Enter**.
4. Respond to the prompts as they appear. Press **Enter** to accept the defaults or type information of your choice and then press **Enter**.

   The information that appears on the screen as you respond to the prompts is self-explanatory and will guide you through the install process.

After you finish installing, open the IWSS Web console and change the admin password to ensure the security of your system (see *Opening the InterScan Web Security Suite Console* on page 3-4 and its subsections).

Opening the InterScan Web Security Suite 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://<domain>:1812/index.jsp`
- `http://<machine name>:1812/index.jsp`
- `http://<IP address>:1812/index.jsp`

See *Accessing the IWSS Console via HTTPS* on page 5-19 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`

Note: The admin password is the primary means of protecting your system from unauthorized access. For a more secure environment, change the console password on a regular basis and use a password that is difficult to guess.

Password Management

The Edit Login Account page is where you can change the user ID and associated password for the administrator and other users. Likewise, you can change the user access rights for a desired login account.

To access the login accounts:

1. Open the IWSS Web console and login with Administrator privileges.
2. Click **Administration > Login Accounts** in the left menu.
3. Click the desired username.

   The Edit Login Account page opens.

Valid Password Characters

The following tips will help you design a safe password:

- Include both letters or special characters as well as numbers in your password
- Avoid words found in any dictionary, of any language
- Intentionally misspell words
- Use phrases or combine words
- Use both uppercase and lowercase letters

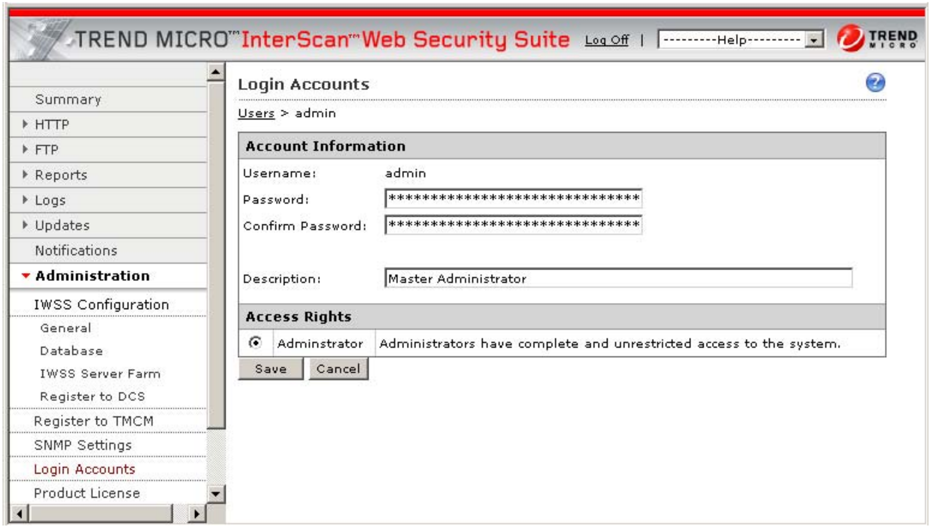
TABLE 3-1. Valid Password Characters

Number	Letters	Special Characters	Special Characters
0-9	A-Z (uppercase) a-z (lowercase)	! (exclamation point)	, (comma)
		“ (double quote)	- (minus or dash)
		# (number sign)	. (period/dot)
		$ (dollar sign)	/ (forward slash)
		% (percent)	: (colon)
		& (ampersand)	; (semi-colon)
		‘ (single quote)	< (less than)
		((left/opening parenthesis)	= (equal sign)
		) (right/closing parenthesis)	> (greater than)
		* (asterisk)	? (question mark)
		+ (plus)	@ (AT symbol)
		[(left/opening bracket)	{ (left/opening brace)
		] (right/closing bracket)	| (vertical bar)
		\ (back slash)	} (right/closing brace)
		^ (caret/cirumflex)	~ (tilde)
		_ (underscore)	‘ (reverse single quote)

Changing Your Password

To change the console password:

1. Open the IWSS Web console and login with Administrator privileges.
2. Click **Administration > Login Accounts** in the left menu.
3. Type your new password in the **Password** field shown in Figure 3-1.
4. Re-type your new password in the **Confirm Password** field.
5. Click **Save**.



Login Accounts

Users > admin

Account Information

Username: admin

Password: ******************************

Confirm Password: ******************************

Description: Master Administrator

Access Rights

● Adminstrator — Administrators have complete and unrestricted access to the system.

FIGURE 3-1. Use a password (password is case-sensitive) that is difficult to guess with 4-32 (preferably at least 8) characters.

Registering the 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 > Register to TMCM > Control Manager Settings page of the IWSS Web console
2. In the Control Manager Settings page, enter the pertinent information.
3. Click **Register**.

   The Connection Manager Status displays: "Registered Control Manager server: Not connected".

   The **Register** button becomes the **Update Settings** button.

   You can only update the MCP Proxy Settings or Two Way Communication Port Forwarding information.

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.

Section 4

Migration Checklist

☑	Step	**Optional**	**Reference**
	Back up the previous version of IWSS		page 4-3
	Back up the Database		page 4-3
	Install the latest version of IWSS		page 3-2
	Change password to confirm a successful installation		page 3-6

Chapter 4

Migrating to InterScan Web Security Suite

This chapter describes how to migrate from a 2.x version of InterScan Web Security Suite to the latest version.

Note: Once you migrate to InterScan Web Security Suite 3.0, you cannot automatically rollback to your previous version.

Note: IWSS no longer supports the use of a local Unix system FTP server. However, if the FTP proxy setting for IWSS 2.x is set to a local Unix system FTP server, then this setting is migrated to IWSS 3.0 as FTP standalone mode. From the **FTP > Configuration > General** page you can view this configuration.

Upgrading InterScan Web Security Suite

You can upgrade your InterScan Web Security Suite 2.x release using the Trend Micro Enterprise Solutions CD or by executing the install script. From the directory containing the untarred IWSS 3.0 package, run the install script. See *Installing InterScan Web Security Suite* on page 3-2.

IWSS automatically detects the existence of IWSS 2.x on your machine and saves your configuration settings. However, while customized directories are saved during the migration, the contents of these directories are not. These directories include the following:

- Reporting and System logs
- Scheduled reports
- Quarantine log

For customized directories, you need to backup and then restore the directory contents if you want to preserve this data in IWSS 3.0. See *Backing Up Directories Prior To Migration* on page 4-4.

Note: The Hacking/Proxy Avoidance category in InterScan Web Security Suite 2.0 release has been split into two separate categories in release 3.0. If you specified this category for an IWSS 2.0 policy, then the migration process will automatically substitute the Proxy Avoidance category in its place. To retain all of the Hacking/Proxy Avoidance category, you must manually select the Hacking category in IWSS 3.0 migrated policies.

Setting the Configuration File

The following are the IPv4 local connection entries in the `pg_hba.conf` file required before migrating from IWSS 2.x:

- IWSS 2.x uses trust mode and IWSS 3.0 uses password mode, which is set during installation. This setting is established for the local database server. For a remote database server, you need to manually set the authentication mode. Specify the following:
  - For a local database: `host all all 127.0.0.1 255.255.255.255 password`
  - For a remote database: `host all all IP_address_of_IWSS 3.0_server 255.255.255.255 password`
- For the local database server, you can use “localhost” or an implicit IP address (for example, 10.2.42.11). If using an implicit IP address, then add an address record in to the `pg_hba.conf` file.

- To allow non-local connections for a remote database server, you need to add more host records. (A *host* is either a plain or SSL-encrypted TCP/IP socket.)
- Before you change the database server authentication mode from "trust" to "password," ensure that the database user has a password. If the database user does not have a password, then this user cannot successful connect to the database.

Saving Customized Settings

Backing Up Your InterScan Web Security Suite 2.x Settings

You can use this backup to manually restore your production InterScan Web Security Suite settings if you want to return to using InterScan Web Security Suite 2.x.

1. Create a ghost image of your machine to retain your InterScan Web Security Suite settings.
2. Execute the following command to backup the database:

   ```
   ./db_backup_2x.sh <HOST_NAME> <DB_PORT> <DB_USER>
   <DATABASE_NAME> <BACKUP_DIR> <BACKUP_TYPE>
   ```

   For example:

   ```
   ./db_backup_2x.sh localhost 5432 sa iwss /var/bk
   all|policy|log
   ```

Backing Up Policy Tables

Policy tables should be backed up for the following reasons:

- To preserve policy configurations in case installation/migration fails. You can reinstall InterScan Web Security Suite and then manually restore the old policy settings in the database. This will reduce the impact of any mishaps.
- The backup policy tables file is needed for migration with a remote database (option 2 in the migration script). Without the policy tables backup file, this migration path would not succeed.

To backup the policy tables, execute the following command from within `iscan`:

```
$/usr/iwss/bin/db_backup_2x.sh <HOST_NAME> <DB_PORT>
<DB_USER> <DATABASE_NAME> <BACKUP_DIR> <BACKUP_TYPE>
```

For example:

```
/usr/iwss/bin/db_backup_2x.sh localhost 5432 sa iwss
/var/bk policy
```

Backing Up Directories Prior To Migration

Trend Micro recommends that the Reporting and System Logs files, Schedule Reports files, and the Quarantine files be backed up prior to performing migration. After migration, you can restore the contents of these directories to the specified directories.

Backing Up Directories for Reporting and System Logs

To back up and restore the log directories:

1. Back up the IWSS 2.x reporting and system log directories.

   The reporting and system log directory paths can be found from the IWSS 2.x **Webconsole Logs > Settings | Reporting Logs tab & System Log tab**.

2. Restore the contents of the IWSS 2.x report directories to the IWSS 3.0 report directory.

Note: The IWSS migration process automatically migrates the following directories from IWSS 2.x: system logs, reporting logs, and quarantine directory. The contents of these directories are not migrated, however.

3. Ensure that the directory structure, permissions, and ownership of the backed up reports file is the same in IWSS 3.0 as it was in IWSS 2.x.

Note: If you restore flat (non-database) log files to IWSS 3.0, these files will not be viewable in the IWSS 3.0 Web console (where logs and reports can be generated) since IWSS 3.0 generates these from the data stored in the database only, and not from flat files. These flat files are can be viewed manually for debugging purposes.

Backing Up the Scheduled Report Directory

To back up and restore the scheduled report directory:

1. Back up the IWSS 2.x scheduled report directory.

   This report directory path can be found from the IIWSS 2.x Web console at **Reports > Customization > Customized the report data maintenance setting | Directory to save the reports.**
2. Restore the IWSS 2.x scheduled report directory to the IWSS 3.0 scheduled report directory.
3. Ensure that the directory structure, permissions, and ownership of the backed up scheduled report file is the same in IWSS 3.0 as it was in IWSS 2.x.

The restored reports can be viewed using the InterScan Web Security Suite Web console (**Reports > Scheduled Reports**) or you can manually open the backed up report directories for viewing.

Backing Up the Directory for the Quarantine Log

To back up and restore the quarantine directory:

1. Back up the IWSS 2.x quarantine directory.

   This quarantine directory path can be found from the IWSS 2.x Web console **Logs > Settings > System Logs | Quarantine** to the IWSS 3.0 Web console **Administration > General | Specify quarantine directory.**
2. Restore the IWSS 2.x quarantine directory to the IWSS 3.0 quarantine directory.
3. Ensure that the directory structure, permissions, and ownership of the backed up quarantine file is the same in IWSS 3.0 as it was in IWSS 2.x.

Note: The information in the quarantine log is encrypted. The contents of the log can be useful if a problem occurs where you need to send TrendLabs information in the log to resolve the problem.

Restoring IWSS 2.x

1. Execute `./uninstall_iwss.sh` in the IWSS 3.x installation package.

   This command automatically removes IWSS 3.0 from the system.

2. Install IWSS 2.x or use the ghost image to restore the entire machine.

   To restore your IWSS configuration, use the ghost image. Otherwise, you will have to manually configure IWSS 2.x.
3. Restore your IWSS 2.x database.
4. Restore any customized directories.

Section 5

Configure Checklist

☑	Step	**Optional**	**Reference**
	Hardware or Non-policy Setup		
	Configure IWSS ICAP (if used)	■	page 5-1
	Bind network to interface card	■	page 5-16
	Set up HTTP Policies		
	Configure HTTP functionality		page 5-24
	Basic Scan Policies		page 5-9
	Java Applet and ActiveX Scanning		page 5-23
	URL Blocking		page 5-12
	Verify URL Filtering Settings		page 5-22
	Ensure IntelliTunnel Security		page 5-35
	Perform LDAP Turning		
	Check tuning for LDAP internal caches	■	page C-3
	Disable verbose logging	■	page C-4
	Testing IWSS		
	Test IWSS post-install configuring		page 5-42
	Run the EICAR test file		page 5-42

Chapter 5

Post-Installation Configuration

This chapter briefly introduces configuration tasks after installing IWSS.

After Installing IWSS ICAP

Perform these post-install configuration steps only if you have installed IWSS ICAP on your system. For non-ICAP users, proceed to *Opening the InterScan Web Security Suite Console* starting on page 3-4.

After installing the IWSS ICAP program files, do the following:

Setting up an ICAP 1.0-compliant Cache Server on page 5-1

Enabling “X-Virus-ID” and “X-Infection-Found” Headers on page 5-9

Setting up an ICAP 1.0-compliant Cache Server

Configure an ICAP client to communicate with the ICAP server.

- *To set up ICAP for NetCache Appliance:* on page 5-2
- *To set up ICAP for the Blue Coat Port 80 Security Appliance:* on page 5-3
- *To set up ICAP for Cisco CE ICAP servers:* on page 5-7

Setting up ICAP for NetCache Appliances

To set up ICAP for NetCache Appliance:

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

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

4. Enter an ICAP license key:
   a. Click the **Setup** tab, and then click **System > Licenses** in the left menu. The **System Licenses** screen appears.
   b. Type **IWFLPWA** under the **ICAP license** section.
   c. Click **Commit Changes**.
5. Select the **Service Farms** tab on the **ICAP 1.0** screen, and then click **New Service Farm** to add ICAP servers. Then, assign the service farm name in the **Service Farm Name** field.
   - For response mode, select **RESPMOD_PRECACHE** in the **Vectoring Point** field
   - For request mode, select **REQMOD_PRECACHE** in the **Vectoring Point** field

   Select **Service Farm Enable**.
6. In the **Load Balancing** field, choose the proper algorithm that you use for load balancing (if you have more than one ICAP server in the service farm). Clear **Bypass on Failure**.

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

7. Under the **Consistency** field, choose **strong** from the drop-down menu and leave the **lbw Threshold** field empty.
8. Under the **Services** text box (for response mode), type:
   `icap://{ICAP-SERVER-IP}:1344/resp on,`
   where `ICAP-SERVER-IP` is the IP address of IWSS ICAP for response mode.

   Under the **Services** text box (for request mode), type
   `icap://{ICAP-SERVER-IP}:1344/REQ-Service on,`
   where `ICAP-SERVER-IP` is the IP address of IWSS ICAP for request mode.

   For multiple IWSS ICAP server services, type the additional entries in step 7. For example:

   For response mode,

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

   Click **Commit Changes**.

   For request mode,

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

   Click **Commit Changes**.

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

9. Click the **Access Control Lists** tab, and then select **Enable Access Control Lists**. Type `icap (Service Farm name of the ICAP Server) any` in **HTTP ACL**. Click **Commit Changes**.

   To configure scanning FTP over HTTP traffic, go to FTP > Configuration > **Access Control Lists**, and then add “`icap (service farm name)`” `any` into the **FTP ACL** field.

Setting up ICAP for Blue Coat Port 80 Security Appliance

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

Log on to the management console by typing http://{SERVER-IP}:8081 in the address bar of your Web browser (specifying port 8081 as the default management port). For example, if the IP address configured during the first-time installation is 123.123.123.12, enter the URL http://123.123.123.12:8081 in the Web browser.

1. Select **Management**. Type the logon user name and password if prompted.
2. Click **ICAP** in the left menu, and then click the **ICAP Services** tab.
3. Click **New**. The **Add ICAP Service** screen appears.
4. In the **ICAP service name** field, type an alphanumeric name. Click **Ok**.
5. Highlight the new ICAP service name and click **Edit**. The **Edit ICAP Service name** screen appears.
6. Type or select the following information:

   a. ICAP version number (that is, 1.0)

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

   - Response mode:

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

   - Request mode:

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

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

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

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

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

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

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

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

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

Note: You can edit the configured ICAP services. To edit a server configuration again, select the service and click **Edit**. The examples used for configuring ICAP for Blue Coat is based on version 2.1.07. The settings may vary depending on the version of Blue Coat.

8. Add response or request mode policy.

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

If you have not installed JRE on your workstation, a security-warning window appears. Click **Yes** to continue. Follow the instructions to install the JRE.

To add the response mode policy:

a. Select **Management**. Type the logon user name and password if prompted.

b. Click **Policy** in the left menu, and then click the **Visual Policy Manager** tab.

c. Click **Start**. If the **Java Plug-in Security Warning** screen appears, click **Grant this session**.

d. On the menu bar, click **Edit > Add Web Content Policy**. The **Add New Policy Table** screen appears.

e. Type the policy name under the **Select policy table name** field. Click **OK**.

f. Under the **Action** column, right-click **Bypass ICAP Response Service** and click **Set**. The **Add Object** screen appears. Click **New** and select **Use ICAP Response Service**. The **Add ICAP Service Action** screen appears.

g. Choose the ICAP service name under the **ICAP Service/Cluster Names** field. Enable **Deny the request** under the **On communication error with ICAP service** section. Click **OK**, and then click **OK** again.

h. Click **Install Policies**.

To add the request mode policy:

a. Select **Management**. Type the logon user name and password if prompted.

b. Select **Policy** in the left menu, and then click the **Visual Policy Manager** tab.

c. Click **Start**. If the **Java Plug-in Security Warning** screen appears, click **Grant this session**.

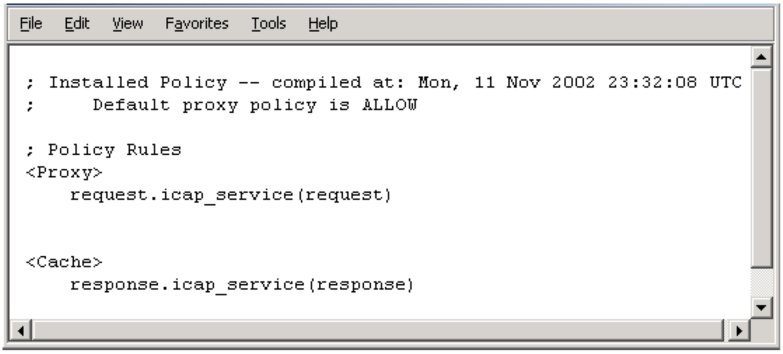
d. On the menu bar, click **Edit > Add Web Access Policy**. The **Add New Policy Table** screen appears.

e. Type the policy name under the **Select policy table name** field. Click **OK**.

f. Under the **Action** column, right-click **Deny** and click **Set**. The **Add Object** screen appears. Click **New** and select **Use ICAP Request Service**. The **Add ICAP Service Action** screen appears.

g. Choose the ICAP service name under the **ICAP Service/Cluster Names** field. Enable **Deny the request** under the **On communication error with ICAP service** section. Click **OK**, and then click **OK** again.

h. Click **Install Policies**.



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

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


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

FIGURE 5-1 Configure both the request and response mode ICAP services. To check the current policy, go to the "Policy" screen, click the "Policy Files" tab, and then click "Current Policy".

Setting up ICAP for Cisco CE ICAP Servers

To set up ICAP for Cisco CE ICAP servers:

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

1. Open the Cisco CE console.
2. Type `config` to enter the configuration mode.
3. Type `ICAP` to display a list of all ICAP-related commands.
4. Create a response modification service, by typing

   ```
   icap service RESPMOD SERVICE NAME
   ```

   This takes you into the ICAP service configuration menu. Display a list of all available commands. Type the following commands:

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

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

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

   `enable` (to enable the ICAP multiple server configuration)
5. Type `exit`.
6. Create a request modification service, by typing

   ```
   icap service REQUESTMOD SERVICE NAME
   ```

   This command takes you into the ICAP service configuration menu. Display a list of all available commands. Issue the following commands:

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

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

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

   `enable` (to enable the ICAP multiple server configuration)
7. Type `exit`.
8. For additional configuration steps, type the following:

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

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

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

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

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

Configuring Virus-scanning Server Clusters

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

To configure a cluster using the management console:

1. Select **Management**. Type the logon user name and password if prompted.
2. Click **ICAP** in the left menu, and then click the **ICAP Clusters** tab.
3. Click **New**. The **Add ICAP Cluster** screen appears.
4. In the **ICAP cluster name** field, type an alphanumeric name. Click **Ok**.
5. Highlight the new ICAP cluster name and click **Edit**. The **Edit ICAP Cluster name** screen appears.
6. Click **New** to add an ICAP service to the cluster. The **Add ICAP Cluster Entry** screen appears. The pick list contains a list of any services available to add to the cluster. Choose a service and click **Ok**.
7. Highlight the ICAP cluster entry and click **Edit**. The **Edit ICAP Cluster Entry name** screen appears. In the **ICAP cluster entry weight** field, assign a weight from 0-255. Click **Ok**, click **Ok** again, and then click **Apply**.

Deleting a Cluster Configuration or Entry

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

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

To delete a cluster configuration using the management console:

1. Select **Management**. Type the logon user name and password if prompted.
2. Click **ICAP** in the left menu, and then click the **ICAP Clusters** tab.
3. Click the cluster you want to delete. Click **Delete**, and then click **Ok** to confirm.

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

IWSS can return 2 optional headers from the ICAP server whenever a virus is found: the “X-Virus-ID” and the “X-Infection-Found” headers. Neither of these headers are returned by default for performance reasons, since many ICAP clients do not use these headers. They must be enabled in the IWSS management console.

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

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

- “X-Infection-Found” returns a numeric code for the type of infection, the resolution, and the risk description.

For more details on the parameter values, see:

`http://www.i-cap.org/spec/draft-stecher-icap-subid-00.txt`

See *Opening the InterScan Web Security Suite Console* on page 3-4 to learn how to access the IWSS management console.

To enable the X-Virus-ID header:

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

HTTP Scanning and General Configuration

After installing IWSS and verifying a successful installation, there are several tasks to prepare the program for your environment. For more information and detailed procedures to perform these tasks, consult the IWSS *Administrator’s Guide*.

Enabling the HTTP Traffic Flow

After installing IWSS and rebooting the server, 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 enable the IWSS HTTP traffic flow:

1. Click **Summary** on the main menu.
2. Click **Turn On** next to **HTTP Traffic**.

Configuring the User Identification Method

IWSS supports several ways to identify clients when configuring a policy’s scope. The default post-install identification method is through the client’s IP address. IWSS also supports identifying clients through their host name or MAC address and through an LDAP directory.

To configure the user identification method:

1. Click **HTTP > Configuration > User Identification** from the main menu.
2. Select the user identification method. If choosing LDAP, enter the LDAP vendor, server and authentication information and test the LDAP connection.
3. Click **Save**.

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 **Guest port number** is 8081 and typically does not have to be modified unless the port is already in use.

4. Click **Save**.

Reviewing Scanning and Filtering Policies

IWSS is pre-configured to provide a baseline level of gateway security. Trend Micro recommends reviewing the HTTP virus scanning Global and Guest policy configurations to ensure they reflect your organization's security policies.

Additionally, if you have installed the Applets and ActiveX security, IntelliTunnel security, URL filtering and FTP scanning modules, review those configurations and modify accordingly.

Reviewing Default Settings

The default IWSS post-install settings are summarized under *Default Post-install Configuration Settings* starting on page 5-24. These settings provide a baseline level of content security that may be appropriate for your organization. Trend Micro recommends that you carefully review the default settings and modify them according to the security needs of your unique environment and overall security goals.

Enabling Access Quota Policies

The default post-install configuration does not apply any access quota. To limit bandwidth consumption, enable access quota control to set a maximum amount of data that a client can retrieve or download during a given time period.

To enable access quota control:

1. Click **HTTP > Access Quota Policies** on the main menu.
2. Select **Enable access quota control**.
3. To configure access quota control for your network's guest users, click **Access Quota Guest Policy** and configure the settings. To configure access quota control for other network users, click **Add** and configure a new policy.
4. Click **Save**.

Configuring Trusted URLs

To minimize performance issues from HTTP scanning, Trend Micro recommends configuring “trusted” URLs to exempt from scanning. For example, if you have configured IWSS in a forward proxy configuration and are confident that your company’s Web site does not harbor any security risks, consider adding it as a trusted site. Other reputable Web sites that are frequently visited by your clients, for example, financial Web sites that provide your company’s stock quote, can also be configured as “trusted”.

To configure trusted URLs

1. From the main menu, click **HTTP > URL Access Control > Trusted URLs**.
2. Select **Do not scan trusted URLs**.
3. Enter or import the URLs, or sub-URLs, to exempt from scanning, along with any exceptions to the trusted URLs.
4. Click **Save**.

Configuring URL Blocking

There may be Web sites that you want to prevent your clients from visiting. URL blocking is enabled by default in the post-install settings, and blocks URLs listed in the PhishTrap pattern file. For detailed instructions on configuring URL blocking, consult the IWSS *Administrator’s Guide*.

To block URLs:

1. Click **HTTP > URL Access Control > URL Blocking** in the main menu.
2. Click **Enable URL blocking**.
3. Enter or import the URLs or sub-URLs to block, along with any exceptions to these blocked URLs.

Setting Access Control Settings

The default IWSS settings allow all non-guest clients to access the Internet. To allow a subset of your clients Internet access, configure the IP addresses allowed to do so on the **Access Control Settings** screen.

In addition, IWSS can be configured to exempt some servers from scanning, URL filtering, and URL blocking to speed up browsing performance when visiting trusted sites. For example, consider adding the IP address ranges of your intranet sites to the Server IP white list to exempt frequently visited sites from scanning and filtering.

To configure which clients are allowed to access the Internet:

1. Click **HTTP** > **Configuration** > **Access Control Settings** from the main menu.
2. On the **Client IP** tab, select **Enable HTTP Access Based on Client IP** and enter the IP addresses that are allowed to access the Internet.
3. On the **Server IP White List** tab, configure the IP addresses of servers that will be exempted from scanning, URL filtering, and URL blocking.
4. Click **Save**.

Configuring Proxy Scan Settings

IWSS is installed in Forward Proxy (Standalone) 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. For detailed information, consult the IWSS *Administrator's Guide*.

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.

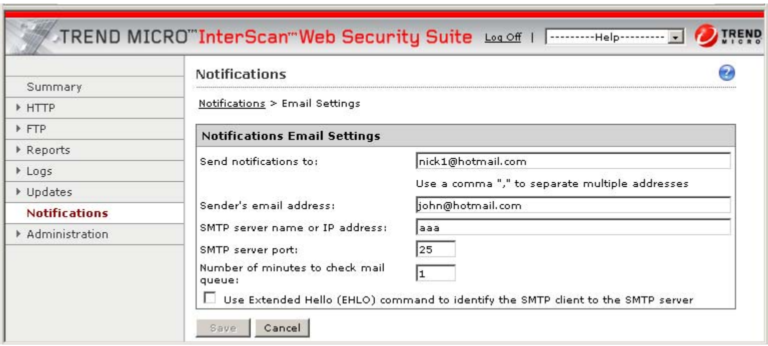
Configuring Notifications

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

Note: 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 review and modify your notification settings:

1. Click **Notifications** on the main menu.
2. Verify that the notification settings for each security and update event match the requirements of your environment.
3. Click **Send notification to** to view and modify the email address or SMTP server to use for notifications.
4. Click **SNMP Notification Settings** to enable or disable sending SNMP traps for certain security, update, or program events.
5. Click **Save**.



Notifications

Notifications > Email Settings

Notifications Email Settings

Send notifications to: nick1@hotmail.com

Use a comma "," to separate multiple addresses

Sender's email address: john@hotmail.com

SMTP server name or IP address: aaa

SMTP server port: 25

Number of minutes to check mail queue: 1

□ Use Extended Hello (EHLO) command to identify the SMTP client to the SMTP server

FIGURE 5-2 Configure email update notifications and SMTP server settings here.

Setting the Database Connection

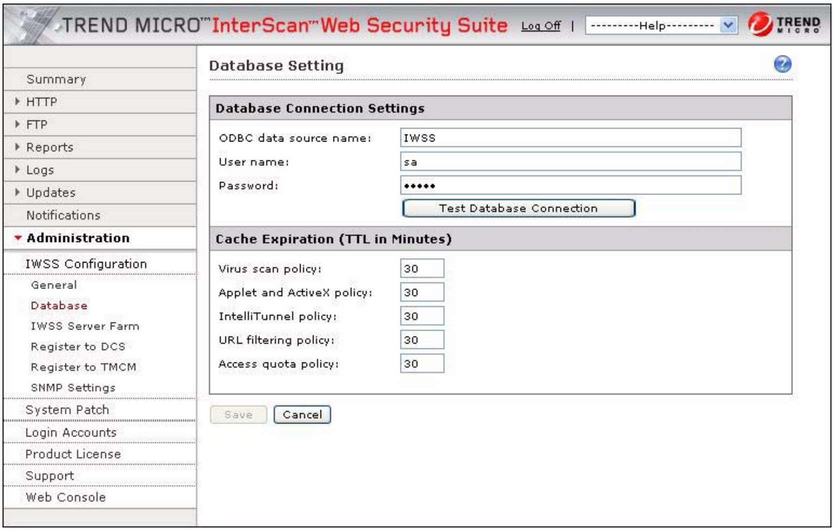
Ensure that you set up your database appropriately under the **Database Connection Settings** section (**Administration > IWSS Configuration > Database**). When you are setting up a database for multiple IWSS server configurations, specify the same database for all IWSS servers. The schema (table definitions, stored procedures, etc.) used by IWSS is initialized during installation.

To configure the database connection settings:

1. Open the IWSS management console and click **Administration > IWSS Configuration > Database**.
2. Under **Database Settings**, type a value for the following parameters:

- **ODBC data source name**
- **User name**
- **Password**

3. Click **Save**.



Database Setting

Database Connection Settings

ODBC data source name: IWSS
User name: sa
Password: •••••

Cache Expiration (TTL in Minutes)

Virus scan policy: 30
Applet and ActiveX policy: 30
IntelliTunnel policy: 30
URL filtering policy: 30
Access quota policy: 30

FIGURE 5-3 To verify that the database connection is working, 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 Cache Expiration in Minutes:

1. Open the IWSS management console and click **Administration > IWSS Configuration > Database**.
2. Under **Cache Expiration (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**.

Configuring the Quarantine Directory

During installation, IWSS creates a quarantine directory (default path = `/etc/iscan/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).

Binding to a Network Interface Card

By default, IWSS binds to all Network Interface Cards (NIC) on the server where IWSS is installed. To have IWSS bind to one NIC only, specify that IP address using the following procedure.

To configure IWSS to listen to a specific network interface:

1. Choose **Administration** > **IWSS Configuration** > **General** from the IWSS main menu.
2. Type the IP address of the network interface to which you want IWSS to bind, and click **Save**.

Changing the Management Console Password

The management 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.

Only administrator-level users can change passwords.

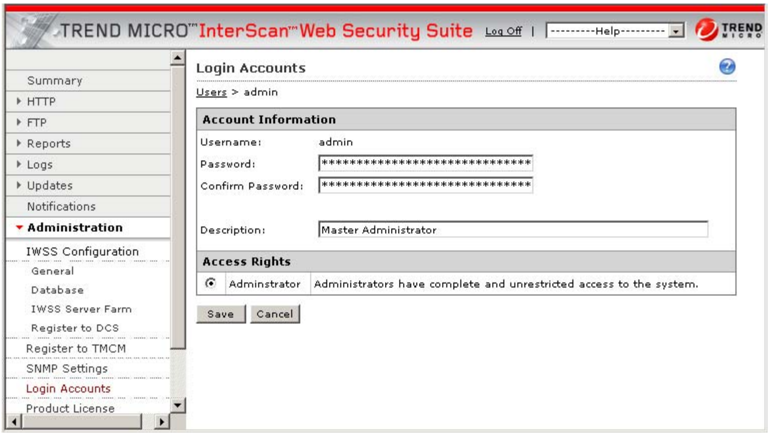
The following tips will help you design a safe password:

- 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 a root 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**.



Login Accounts

Users > admin

Account Information

Username: admin

Password: ******************************

Confirm Password: ******************************

Description: Master Administrator

Access Rights

● Adminstrator Administrators have complete and unrestricted access to the system.

Save Cancel

FIGURE 5-4 Use a difficult password (password is case-sensitive) with 4-32 alphanumeric characters

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 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/AdminUI/jre/bin` (the default install directory is `/opt/trend/`).

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

1. Execute the following from a terminal command line:

   ```
   ./keytool  -genkey -alias tomcat -keyalg RSA
   -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. Copy the mykeystore file into the Tomcat base directory, renaming it `keystore.tmp`:

`cp /etc/iscan/AdminUI/jre/bin/mykeystore` to `/etc/iscan/AdminUI/tomcat/keystore.tmp`

4. From the Administration > Web Console page, enter the SSL password used to create the mykeystore file.
5. Enter the port number you wish to use for the SSL connection and then save this information.
6. 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.
7. Go to URL `https://hostname:port` and specify the correct port.
8. Stop and restart the `IWSS_UI` daemon.
9. 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`
10. To enable the certificate, go to `/etc/rcX.d` (where X is the run level number of the installed host) of the IWSS server to manually restart `S99IScanHttpd`:

    ```
    ./S99IScanHttpd stop
    ./S99IScanHttpd start
    ```

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 `/etc/iscan/AdminUI/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 `/etc/rcX.d` (where X is the run level number of the installed host) of the IWSS server to manually restart `S99IScanHttpd`:

```
./S99IScanHttpd stop
./S99IScanHttpd start
```

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
```

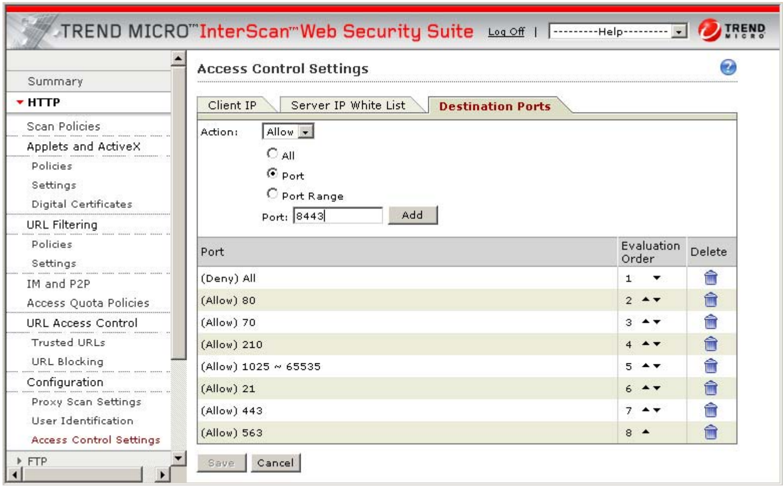
Using SSL with Damage Cleanup Services (DCS)

To redirect clients to DCS to clean up malicious code when you are using the HTTPS-enabled Web management console, access to the secure port that IWSS uses (typically 8443) must be enabled. Otherwise, redirection to DCS will not be successful, since the redirection request will be blocked.

To allow access to secure port 8443:

1. Click **HTTP > Configuration > Access Control Settings**, and make the **Destination Ports** tab active.
2. Under the Action drop-down list, select **Allow.**
3. Select the **Port** radio button.
4. In the **Port** field, enter the port number used for HTTPS traffic (typically 8443).

5. Click **Add** and then **Save**.



Access Control Settings

Action: Allow

○ All
● Port
○ Port Range

Port: 8443 Add

Port	Evaluation Order	Delete
(Deny) All	1 ▼	🗑
(Allow) 80	2 ▲▼	🗑
(Allow) 70	3 ▲▼	🗑
(Allow) 210	4 ▲▼	🗑
(Allow) 1025 ~ 65535	5 ▲▼	🗑
(Allow) 21	6 ▲▼	🗑
(Allow) 443	7 ▲▼	🗑
(Allow) 563	8 ▲	🗑

FIGURE 5-5 Allow access to the secure port (typically 8443) if using DCS and the HTTPS management console

In addition, two parameters in the `[http]` section of the `intscan.ini` file need to be modified when IWSS is configured to use HTTPS:

```
iscan_web_server=[user defined https port, e.g., 8443]
```

```
iscan_web_protocol=https
```

Verifying URL Filtering Settings

InterScan Web Security Suite includes a database that contains URLs in over 60 categories, such as “gambling,” “games,” and “personals/dating.” Categories are segmented in seven logical groups. By default, no categories are pre-selected.

Trend Micro recommends reviewing the URL filtering settings to ensure the categories that qualify as company prohibited sites reflect the values of your organization and do not impact your employee’s business-related Web browsing. For example, a clothing retailer may need to remove the “Intimate Apparel/Swimsuit” category from the “company prohibited sites.” Additionally, you may need to configure URL exceptions to enable employee access to specific sites that would otherwise be blocked, and review the definitions of “work time” to ensure it reflects your workplace schedule.

To review URL filtering settings:

1. Click **HTTP > URL Filtering > Settings** from the main menu.
2. On the **URL Filtering Exceptions** tab, enter or import Web sites to exempt from URL filtering so that they will always be accessible to your clients.
3. On the **Schedule** tab, the default setting for “work time” is Monday to Friday, from 8:00 to 11:59, and from 13:00 to 17:00. Modify these time settings according to employee schedules in your workplace.

Java Applet and ActiveX Scanning

Java applet signatures are verified using root certificates installed during IWSS setup—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 server’s certificate store.

Adding Certificates for Applet Signature Verification

If your environment requires running applets signed with root certificates that are not installed along with IWSS, 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 **Manage Digital Certificates** screen and verify the added certificate displays in the list.

Default Post-install Configuration Settings

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

TABLE 5-1. Default Post-install IWSS Settings

Configuration	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 \IWSS\Quarantine in the install folder
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 • Decompressed size 100 times greater than compressed file size **Large file scanning**: • Files greater than 2048MB are not scanned • Files greater than 512KB are scanned using deferred scanning **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 5-1. Default Post-install IWSS Settings

Configuration	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 11:50 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 5-1. Default Post-install IWSS Settings

Configuration	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 • Decompressed size more than 100 times the compressed file size **Large file scanning**: • Files greater than 1024MB are not scanned • Deferred scanning is enabled for files greater than 512KB **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 and log files, and kept for 30 days • Reporting logs include performance data • System logs are written to the \IWSS\Log folder, and kept for 5 days
Updates	• Check for virus, spyware, and PhishTrap pattern updates hourly • Check for scan engine updates weekly • Check for URL filtering database updates weekly
Notifications	**Enabled email notifications**: • HTTP file blocking events • URL blocking events • Virus, PhishTrap, spyware pattern updates and URL filtering database (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 off by default • DCS is enabled (but must configure IP address and port of DCS server)
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 `/etc/hosts` file so that the host name does not resolve to 127.0.0.1.

Configuring an IWSS Server Farm

Multiple IWSS servers can be installed to balance traffic and scanning loads. In a multiple server configuration, one server is designated as the “master” and the master’s configuration is used for all the IWSS servers in the farm. 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 servers on their network.

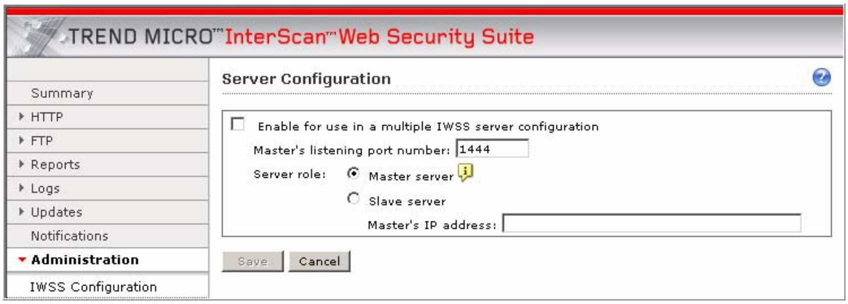
To configure server designation:

1. Open the IWSS management 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.

WARNING! *A group of IWSS servers must have one, and only one, master server.*

5. Click **Save**.



□ Enable for use in a multiple IWSS server configuration

Master's listening port number: 1444

Server role: ● Master server ○ Slave server

Master's IP address:

FIGURE 5-6 Configuring the server's role, either master or slave, in the Server Configuration screen

Updating Program Components

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

New versions of the Trend Micro scan engine are updated as performance is improved and features added to address new risks. The URL filtering database is updated as new Web sites are launched and their content categorized.

Note: If Internet connections on your network pass through a proxy server and you did not configure your proxy information during install, click **Updates > Connection Settings** from the main menu and enter your proxy server information.

To update the pattern files, scan engine and URL filtering database:

1. Click **Summary** on the main menu and make sure the **Scanning** tab is active.

2. For all of the components listed on the **Scanning** tab, select components to update and click **Update**.

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

The following components in IWSS are updatable:

- *Updating the Virus Pattern File* on page 5-29
- *Updating the PhishTrap Pattern File* on page 5-32
- *Updating the Spyware Pattern File* on page 5-33
- *Updating the Scan Engine* on page 5-34
- *Updating the URL Database (for URL Filtering Option Only)* on page 5-34
- *Updating the IntelliTunnel Signatures* on page 5-35

Updating the Virus Pattern File

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

All Trend Micro antivirus programs using the ActiveUpdate feature can detect whenever a new virus pattern is available at the server, and/or can be scheduled to automatically poll the server every hour, day, week, etc. to get the latest file. Trend Micro recommends that you schedule automatic updates to occur no less often than once a week. Virus pattern files can also be manually downloaded from the following Web site:

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

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

How it Works

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

Note: ActiveUpdate also supports incremental updates. Rather than download the entire five or six megabyte file each time, the ActiveUpdate feature can download only the portion of the file that is new and append it to the existing pattern file. Especially for networks running hundreds of individual desktop products, ActiveUpdate can save considerable bandwidth.

Pattern files use the following naming format:

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

where ### stands for 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 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 virus pattern files on a regular basis (sometimes several times per week), and recommends you to set a daily automatic update. Updates are available to registered IWSS users.

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

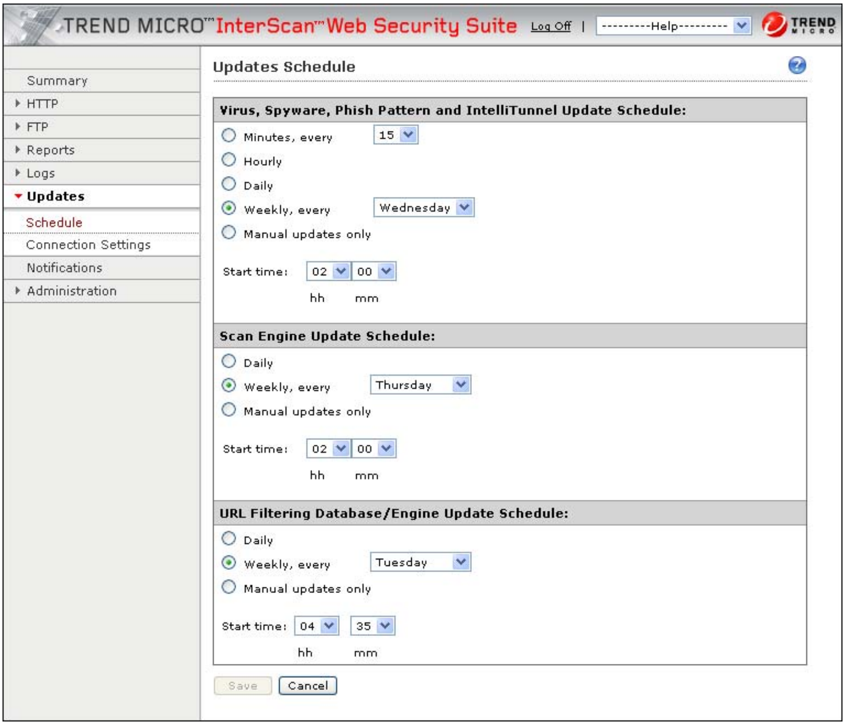
To manually update the virus pattern file:

1. Open the IWSS console and click **Summary** in the left menu.
2. Select **Virus pattern** under the **Component** column and click **Update**. A progress bar appears to indicate the update progress, and a message screen then displays the outcome of your update.

To schedule automatic virus pattern, spyware, and PhishTrap updates:

1. Open the IWSS console and click **Updates > Schedule**.
2. Under the **Virus, Spyware, Phish Pattern and IntelliTunnel Update Schedule** section, select from the following options:
   - Minutes (15, 30, 45, 60)
   - Hourly
   - Daily (recommended setting)
   - Weekly (select a day from the drop-down menu)
   - Manual updates only
3. In the **Start time** field, select the start time from the drop-down menu.
4. Click **Save**.

Note: Use the **Summary > Scanning tab** screen in the IWSS console to verify the current version of the virus 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 virus pattern file to ensure that no viruses are being cached.



Updates Schedule

Virus, Spyware, Phish Pattern and IntelliTunnel Update Schedule:

○ Minutes, every 15
○ Hourly
○ Daily
● Weekly, every Wednesday
○ Manual updates only

Start time: 02 hh 00 mm

Scan Engine Update Schedule:

○ Daily
● Weekly, every Thursday
○ Manual updates only

Start time: 02 hh 00 mm

URL Filtering Database/Engine Update Schedule:

○ Daily
● Weekly, every Tuesday
○ Manual updates only

Start time: 04 hh 35 mm

FIGURE 5-7. Automatically scheduled Virus, Spyware, PhishTrap pattern files, Scan Engine, URL Filtering Database, and IntelliTunnel Update Schedules configured via the IWSS console.

Updating the 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 `/etc/iscan/`. The `PhishB.ini` file, which contains a list of phishing URLs, is encrypted and is maintained and encoded by TrendLabs.

To manually update the PhishTrap pattern file:

1. Open the IWSS console and click **Summary** in the left menu.
2. Select the **Scanning** tab.
3. Select **Phish pattern** under the **Component** column.
4. Click **Update**.

   A progress bar appears to indicate the update progress, and a message screen then displays the outcome of your update.

Updating the Spyware Pattern File

As new hidden programs (spyware) 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 pattern file. The spyware pattern file, which is stored in `/etc/iscan/`, uses the following naming format:

```
ssaptn.###
```

where ### stands for the pattern version. This format provides for a given pattern file with the same pattern version and a different build number. It also accommodates pattern versions greater than 999. The IWSS console displays the following format:

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

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

To manually update the spyware pattern file:

1. Open the IWSS console and click **Summary** in the left menu.
2. Select the **Scanning** tab.
3. Select **Spyware pattern** under the **Component** column
4. Click **Update**.

A progress bar appears to indicate the update progress, and a message screen then displays the outcome of your update.

Updating the Scan Engine

The IWSS scan engine is updated with new features and improvements and posted for download on the Trend Micro Web site. You can update the scan engine manually or automatically.

To manually update the scan engine:

1. Open the IWSS console and click **Summary** in the left menu.
2. Select the **Scanning** tab.
3. Select **Scan engine** under the **Component** column
4. Click **Update**.

   A progress bar appears to indicate the update progress, and a message screen then displays the outcome of your update.

To schedule automatic scan engine updates:

1. Open the IWSS console and click **Updates > Schedule**.
2. Under the **Scan Engine Update Schedule** section, select from the following options:
   - Daily
   - Weekly, every (select from the drop-down menu the day of the week)
   - Manual updates only
3. In the **Start time** field, select the start time from the drop-down menu.
4. Click **Save**.

Updating the URL Database (for URL Filtering Option Only)

The URL database (for URL filtering option only) is updated with the latest list of Web pages, which were grouped into different categories (Company Prohibited Sites, Not Work Related, Possible Research Topics, Business Function Related, Customer Defined, and Others). You can update the URL filtering database and URL filtering database engine manually or automatically (either daily or weekly).

To manually update the URL filtering database:

1. Open the IWSS console and click **Summary** in the left menu.
2. Select the **Scanning** tab.
3. Select **URL filtering database** or **URL filtering database engine** under the **Component** column
4. Click **Update**.

   A progress bar appears to indicate the update progress, and a message screen then displays the outcome of your update.

To schedule automatic URL filtering database updates:

1. Open the IWSS console and click **Updates > Schedule**.
2. Under the **URL Filtering Database/Engine Update Schedule** section, select from the following options:
   - Daily
   - Weekly, every (select from the drop-down menu the day of the week)
   - Manual updates only
3. In the **Start time** field, select the start time from the drop-down menu.
4. Click **Save**.

Updating the IntelliTunnel Signatures

To manually update the IntelliTunnel signatures:

1. Open the IWSS console and click **Summary** in the left menu.
2. Select the **Scanning** tab.
3. Select **IntelliTunnel signatures** under the **Component** column
4. Click **Update**.

   A progress bar appears to indicate the update progress, and a message screen then displays the outcome of your update.

Rolling Back to Previous Component Versions

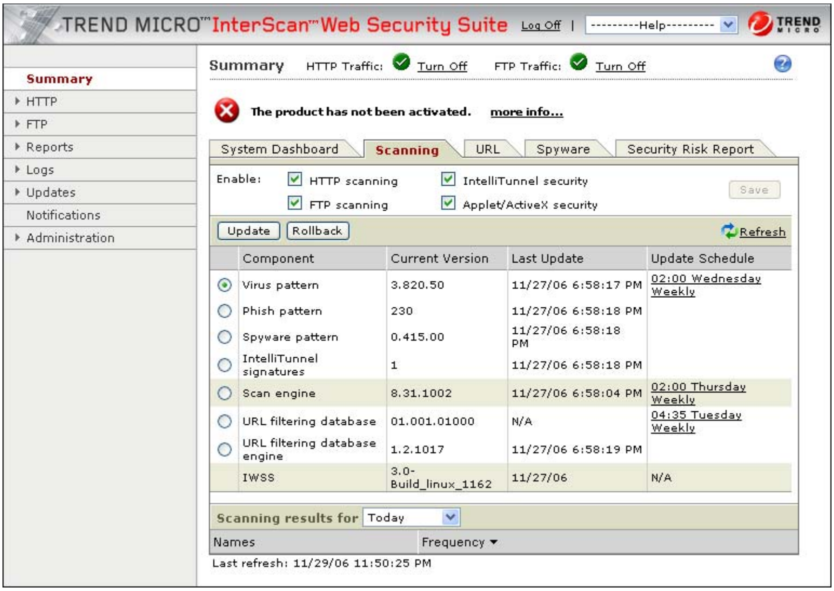
IWSS looks in the program directory and uses the latest pattern file and engine library file (`libvsapi.so`) to scan inbound/outbound traffic. It can distinguish the latest pattern file by its file extension; for example, lpt$vpn.401 is newer than lpt$vpn.400.

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 by clicking the **Rollback** button.

To manually rollback the scan engine, PhishTrap, Spyware, IntelliTunnel, or virus pattern file:

1. Open the IWSS console and click **Summary** in the left menu.
2. Select the **Scanning** tab.
3. Select the appropriate component and click **Rollback**.

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



Summary HTTP Traffic: ✓ Turn Off FTP Traffic: ✓ Turn Off

☒ The product has not been activated. more info...

Enable: ☑ HTTP scanning ☑ IntelliTunnel security
☑ FTP scanning ☑ Applet/ActiveX security

	Component	Current Version	Last Update	Update Schedule
●	Virus pattern	3.820.50	11/27/06 6:58:17 PM	02:00 Wednesday Weekly
○	Phish pattern	230	11/27/06 6:58:18 PM	
○	Spyware pattern	0.415.00	11/27/06 6:58:18 PM	
○	IntelliTunnel signatures	1	11/27/06 6:58:18 PM	
○	Scan engine	8.31.1002	11/27/06 6:58:04 PM	02:00 Thursday Weekly
○	URL filtering database	01.001.01000	N/A	04:35 Tuesday Weekly
○	URL filtering database engine	1.2.1017	11/27/06 6:58:19 PM	
	IWSS	3.0-Build_linux_1162	11/27/06	N/A

Scanning results for Today

Names Frequency ▾

Last refresh: 11/29/06 11:50:25 PM

FIGURE 5-8. You can only perform a Virus pattern, Phish pattern, Spyware pattern, IntelliTunnel, and Scan engine

version rollback to one version lower than your existing current version.

Note: The URL filtering database does not support rollback.

Forced Update Option

IWSS provides an option to force an update to the pattern file and the scan engine when the version is greater than or equal to its counterpart on the remote download server. The feature is useful when a new pattern or scan engine is found to be corrupted and an older version is temporarily used to replace the ineffective one on the remote download server.

To force the update of the pattern file and scan engine:

1. Open the IWSS console and click **Summary** in the left menu.
2. Click the **Scanning** tab.
3. Select the component's radio button, and then click **Update**. A pop-up window appears if the version of the pattern file or scan engine on the IWSS server is greater than or equal to the counterpart in the remote download server.
4. Click **Save** to do a forced update.

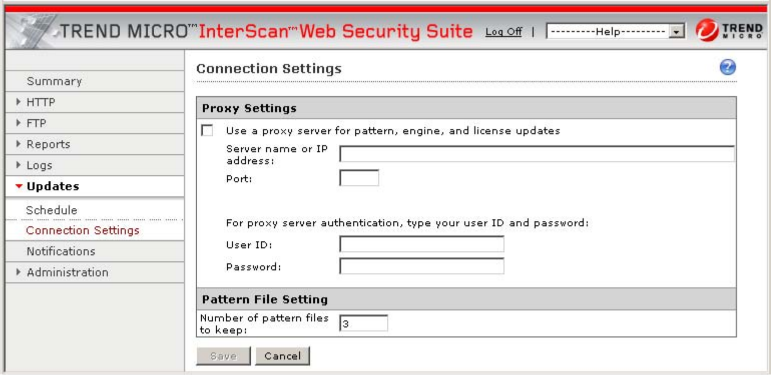
Proxy Settings for Pattern, Engine, and License Updates

If you use a proxy server to access the Internet, configure your proxy server for pattern, engine and license updates.

To configure a proxy server for pattern, engine, and license updates:

1. Open the IWSS console and click **Updates > Connection Settings**.
2. Click **Use a proxy server for pattern, engine, and license updates**. Type the server name and port number in the fields provided.
3. If your proxy server requires authentication, then type your user ID and password in the fields provided.

4. In the **Pattern File Setting** section, type the number of pattern files to keep.
5. Click **Save**.



Connection Settings

Proxy Settings

☐ Use a proxy server for pattern, engine, and license updates

Server name or IP address:

Port:

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

User ID:

Password:

Pattern File Setting

Number of pattern files to keep: 3

FIGURE 5-9. **If your proxy server requires authentication, type a user ID and password in the fields provided.**

Update Notification Settings

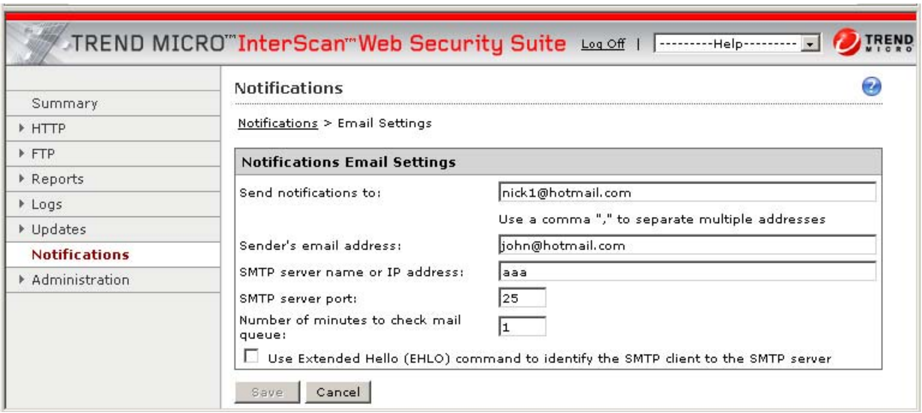
IWSS gives you the option to receive notification status messages about virus, PhishTrap, spyware, scan engine, or URL filtering database updates.

To configure update notifications:

1. Open the IWSS console and click **Updates > Notifications**.
2. You can configure the email settings by clicking **Send Notification to...** on the **Notifications** screen. Type a value for each of the following configuration fields:
   - Email address of the receiver of the notification messages in the **Send notification to** field. Use a comma as a delimiter for multiple email addresses
   - Email address of the sender of the notification messages in the **Sender's email address** field
   - SMTP server name or the IP address of the mail server that will send the notification messages in the **SMTP server name or IP address** field (the default is localhost). This email server must be configured to accept relayed messages from the IWSS installation server

- Port used by the mail server, typically 25, in **SMTP server port**
- Frequency that the mail queue must be checked in the **Number of minutes to check mail queue** field.
- If necessary, select the checkbox for **Use Extended Hello (EHLO) command to identify the SMTP client to the SMTP server.**

3. Click **Save**.



Notifications

Notifications > Email Settings

Notifications Email Settings

Send notifications to: nick1@hotmail.com

Use a comma "," to separate multiple addresses

Sender's email address: john@hotmail.com

SMTP server name or IP address: aaa

SMTP server port: 25

Number of minutes to check mail queue: 1

☐ Use Extended Hello (EHLO) command to identify the SMTP client to the SMTP server

FIGURE 5-10. Use this screen to configure update notifications.

Activating IWSS and URL Filtering

You can activate IWSS during the installation process or later using the IWSS console. URL filtering, however, is activated using the IWSS console. To activate IWSS and URL filtering, you need to have two different Activation Codes.

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:

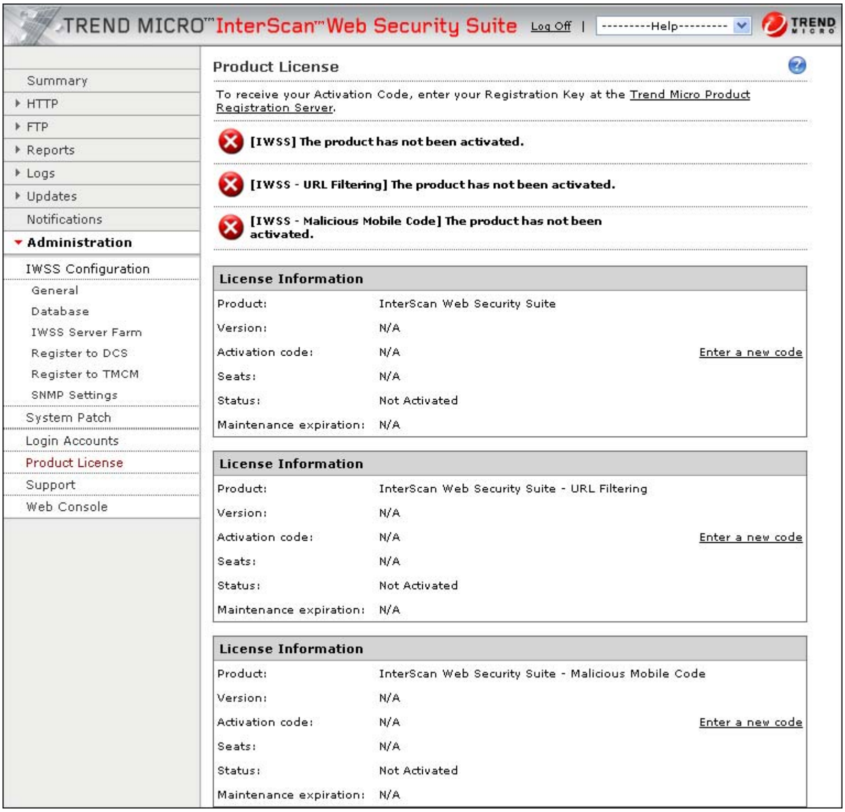
- Trend Micro Enterprise Solutions CD
- License Certificate (which you obtained after purchasing the product)

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

- Updates to the IWSS virus pattern file, spyware and PhishTrap pattern files and scan engine
- Updates to the URL filtering database
- 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 (see Figure 5-11), you can obtain an Activation Code online, view renewal instructions, and verify the status of your product.



Product License

To receive your Activation Code, enter your Registration Key at the Trend Micro Product Registration Server.

[IWSS] The product has not been activated.

[IWSS - URL Filtering] The product has not been activated.

[IWSS - Malicious Mobile Code] The product has not been activated.

License Information		
Product:	InterScan Web Security Suite	
Version:	N/A	
Activation code:	N/A	Enter a new code
Seats:	N/A	
Status:	Not Activated	
Maintenance expiration:	N/A	

License Information		
Product:	InterScan Web Security Suite - URL Filtering	
Version:	N/A	
Activation code:	N/A	Enter a new code
Seats:	N/A	
Status:	Not Activated	
Maintenance expiration:	N/A	

License Information		
Product:	InterScan Web Security Suite - Malicious Mobile Code	
Version:	N/A	
Activation code:	N/A	Enter a new code
Seats:	N/A	
Status:	Not Activated	
Maintenance expiration:	N/A	

FIGURE 5-11. In the “Product License” screen, click “Enter a new code” to upgrade from evaluation to full version.

To obtain an Activation Code online:

1. Open the IWSS console and click **Administration > Product License**.
2. Click **Trend Micro Product Registration Server**. 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.

Testing IWSS with the EICAR Test Virus

After installing IWSS, verify that the application is working properly.

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 virus pattern file from most antivirus vendors. The test virus is not a virus and does not contain any program code.

WARNING! *Never use real viruses to test your 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.

To further verify the IWSS installation, access Appendix D, *Additional IWSS Testing* and test the following functionary:

- Upload scanning
- FTP scanning
- URL blocking
- Download scanning
- URL filtering
- Spyware scanning
- PhishTrap scanning
- Applet and ActiveX scanning
- IntelliTunnel blocking

Appendix A

Deployment Planning and Staging

This chapter describes the planning and stage phases of deploying IWSS. Topics in this chapter include:

Planning and Staging Overview

Some planning decisions must be made before attempting to install IWSS. This chapter provides necessary information in that step. It includes information about your database options, reports and logs, accepted user ID mechanisms and traffic flow planning.

Staging a test deployment involves choosing a test environment, creating a rollback plan, and how to deploying and evaluate IWSS.

Planning Your Report and Log Setup

IWSS provides statistics on traffic usage on the network, which over time helps you construct a long-term network traffic profile. The report helps you to optimize the network and its security.

IWSS gives you the option of generating reports based on a given category of specific user(s), all users, all groups, or specific group(s). You can either create the report manually (real-time) or automatically (scheduled). Also, you can send the report notification to the email addresses defined in the configuration setting at given time intervals (daily, weekly, or monthly).

You have the option of writing the reporting logs to database and text files or database only. Configure this option in the IWSS console under **Logs > Settings > Reporting Logs**. The text logs are available for compatibility with previous IWSS versions and to further analyze the log data using custom scripts or other third-party applications. They can also be used to validate the completeness and accuracy of logging to the database.

Trend Micro recommends migrating previous version settings to “database only.” IWSS writes data to the database at a configurable interval. Reports and database logs will not reflect the activity since the last database import.

There is a performance penalty for enabling the access log (**Log HTTP/FTP access events** is disabled by default). However, many reports on user activities will not be available if the access log is disabled. Moreover, if IWSS is configured as an upstream proxy, valuable data on user activities may not be available to IWSS. For IWSS to record Internet access activities, the access log must be enabled under **Logs > Settings > Reporting Logs > Options**.

The IWSS management console displays the graphs (Bar, Stacked bar, or Line) and statistics of a generated report. In addition, you can export data from IWSS logs for further analysis using Microsoft Excel. To query and generate reports dynamically, IWSS uses an efficient database management system that can support other major databases as a plug-in.

Planning Your User ID Mechanism

IWSS allows administrators to create IWSS policies that enforce organizational policies regarding acceptable use of its Internet resources. It enforces these policies on either a global or user-by-user basis.

To enforce policies on a user-by-user basis, IWSS requires some mechanism for distinguishing which user is making an HTTP request. IWSS supports four user identification methods to configure policies and trace events back to clients:

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

This choice controls the information that IWSS includes in the virus log, Internet access log, and URL blocking and filtering logs.

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.

Using IP Addresses

Identifying users by the client IP address is the simplest of the mechanisms. This is because IWSS can always determine the IP address of the client making the HTTP proxy request.

The IP address identification option requires that IP addresses are not dynamically assigned via Dynamic Host Configuration Protocol (DHCP) and that network address translation (NAT) is not performed on the network path between the affected system and IWSS. If the local network meets these conditions, configure IWSS to log the IP address information. No further action is required.

Administrators should only rely on IP addresses for identifying users if all of the following are true:

- 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 other

With this mechanism, administrators can create policies based on individual IP addresses, or ranges of IP addresses. For example, an administrator can establish a small quota and tight Web access for machines in a guest area, while others have no quota and more liberal access to Web sites.

Using Host Names

Identifying users by hostname 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:

- 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 <INSTDIR>\HTTP. 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 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 200X servers, 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 A-1. 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 Admin 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.

For more information about user identification and LDAP directory authentication, consult chapter 4 of the IWSS *Administrator's Guide*.

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.

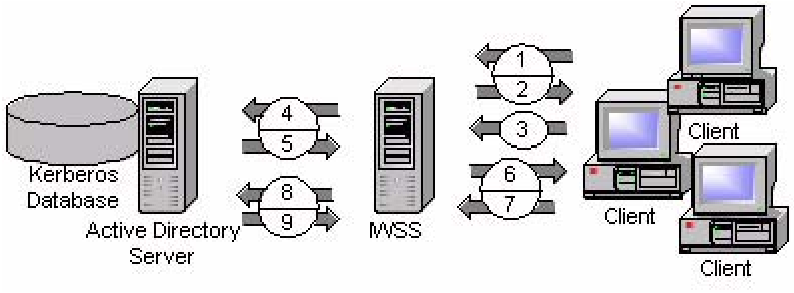


FIGURE A-1. LDAP server authentication workflow (Active Directory shown)

The following steps explain the authentication workflow for Active Directory (AD) shown in Figure A-1. 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 A-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.

Planning Network Traffic Protection

To enforce the network traffic protection using IWSS, an additional solution (hardware, software or configuration) must be introduced that redirects the HTTP and/or FTP traffic to IWSS. Those solution include:

- *Reconfiguring Client Settings* starting on page A-10
- *Using a Layer 4 Switch* starting on page A-11
- *Using an ICAP-enabled Proxy* starting on page A-12

Reconfiguring Client Settings

HTTP clients (browser or proxy servers) can be configured to contact IWSS as a proxy. This configuration ensures that the FTP-over-HTTP traffic is forwarded to IWSS. The HTTP scanning service must be installed in the HTTP Proxy mode to process this traffic.

Set the following parameters in the [http] section of the pni file:

• `transparency= no`	Disables transparent mode
• `self_proxy= (yes|no)`	Depends on the traffic delivery requirements

FTP clients must contact IWSS instead of the destination server, and use a modified handshake to supply the FTP server address. The FTP scanning module must be installed and configured in standalone mode (`proxy_mode=standalone`) to process this traffic.

TABLE A-2. Reconfiguring the Client Settings

Advantage	Limitation
No additional hardware required	Administrator have to control settings for all computers. (Guest computers can have difficulties.)

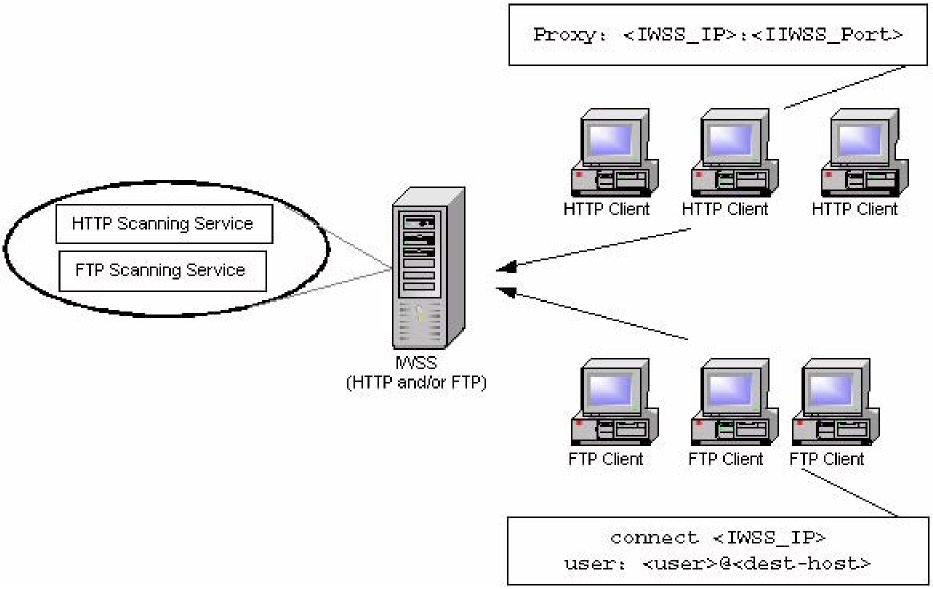


FIGURE A-2 Reconfiguring the Client Settings

Using a Layer 4 Switch

A Layer 4 switch can be used to redirect HTTP traffic to IWSS. The HTTP Scanning Service must be installed in the HTTP Proxy mode.

Set the following parameters in the [http] section of the pni file:

- `transparency=simple` enables simple transparent mode
- `self_proxy yes|no` based on traffic delivery requirements

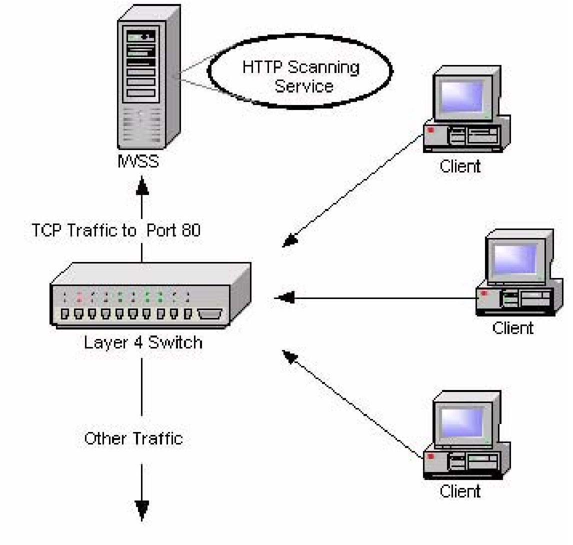


FIGURE A-3 Using a Layer 4 Switch

TABLE A-3. Using a Layer 4 Switch

Advantages	Limitations
Transparent to clients	Traffic interception must be port based (not protocol based) for one port. If the non-standard port is used for HTTP, it bypasses the switch.
Simple to establish	The switch-based redirection cannot be used for the FTP traffic.
	No LDAP support

Using an ICAP-enabled Proxy

Internet Content Adaptation Protocol (ICAP) is designed to forward HTTP response/request to third-party processors and collect the result. The component that sends the ICAP request is called the ICAP-client. A component that processes the request is called an ICAP-server.

When IWSS is configured in ICAP mode, it processes requests from any ICAP-compliant client. Officially, Trend supports the following ICAP implementations: NetCache, Blue Coat, and Cisco Content Engines (CE).

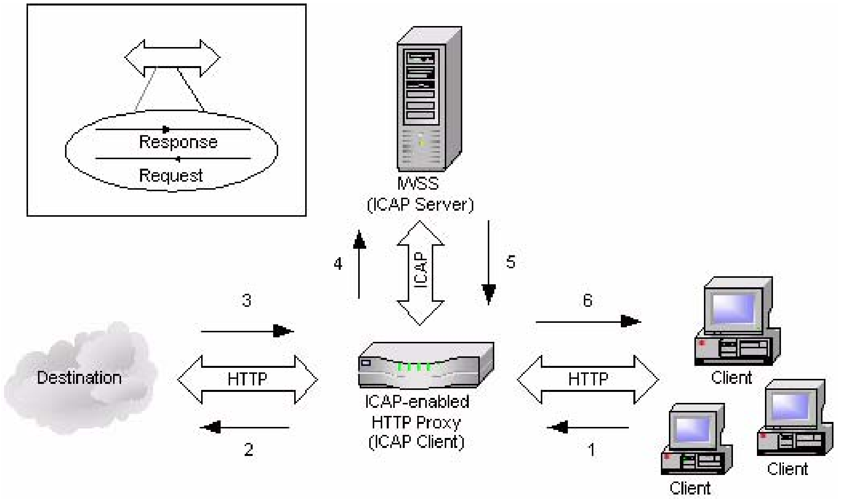


FIGURE A-4 Using an ICAP-enabled Proxy

TABLE A-4. Using am ICAP-enabled Proxy

Advantages	Limitations
ICAP allows scanning of only new and necessary content.	Up front coast of ICAP resources
Reduced, selective scanning enhances performance	Adds extra step in IWSS installation process
Increased resource efficiency reduces the number of IWSS server hardware needed	Requires management.

Planning HTTP and FTP Service Flows

Each HTTP and FTP configuration has implications for configuring IWSS, configuring the network, and for network security.

Create a flow plan for the HTTP and FTP services by doing the following:

- Understand each IWSS services purpose and function
- Determine each service's valid data sources. For example, does the HTTP service receive requests directly from the HTTP browsers, or indirectly through an ICAP proxy device?
- Determine which ports to use for the service. For instance, by default, the HTTP service uses port 8080, and the FTP service uses port 21. However, if another application or service is using port 8080, the administrator must configure the HTTP service to use a different port.
- Determine each services valid data destinations. For example, does the HTTP service send validated requests directly to the Web site? Or, does the HTTP service send the validated request to an upstream HTTP proxy?
- Add in any service-specific considerations. For instance, the HTTP service flow might include an ICAP device, but the FTP service flow does not.

Using the information gathered above, administrators determine which one of the possible flows to use for the installation.

Planning the HTTP Flow

The first step when planning HTTP flow for IWSS is choosing the type of handler:

- HTTP Proxy
- ICAP device

The flow involving an ICAP device is very different from those that do not involve ICAP devices.

There are five main possible flows:

For Forward Proxy Settings:

- **Standalone mode**—Use this flow when ICAP devices are not being used with IWSS, and IWSS connects directly to the Internet. This is the default flow created during installation.

- **Dependent mode**—Use this flow when ICAP devices are not being used with IWSS, and IWSS cannot connect directly to the Internet, but must instead connect through another HTTP proxy. This is can be accomplished in two ways:
    - Proxy-ahead mode
    - Proxy-behind mode (not recommended)
    - Double-proxy mode
- **Transparent proxy mode** - Use this mode when clients computers are not configured to use the IWSS server as their default gateway, but still need to connect to the Internet through IWSS

For reverse proxy settings:

- **Reverse proxy mode—**Use this flow to protect a Web server with a proxy server by placing the HTTP proxy between the Internet and the Web server. (Used by ISPs and ASPs to protect the upload traffic against viruses and by organizations with complex Web sites that need a centralized point of access control.)

For ICAP proxy settings:

- **ICAP protocol mode**—Use the ICAP protocol flow to use ICAP devices with IWSS

Each configuration has implications for configuring IWSS, configuring the network, and for network security.

HTTP Proxy in Standalone Mode

For HTTP browsers to use this flow, configure the browsers to proxy through the IWSS serve (default port 8080).

Web page requests follow this sequence:

1. The Web client sends a request to the HTTP service.
2. The HTTP service validates the request, if the URL is not blocked. If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction. If the URL is valid, the HTTP service attempts to connect to the applicable Web server.
3. The contacted Web site returns a response from the Web server to the HTTP service.

4. The HTTP service scans the content for unwanted data and returns the appropriate response to the client.

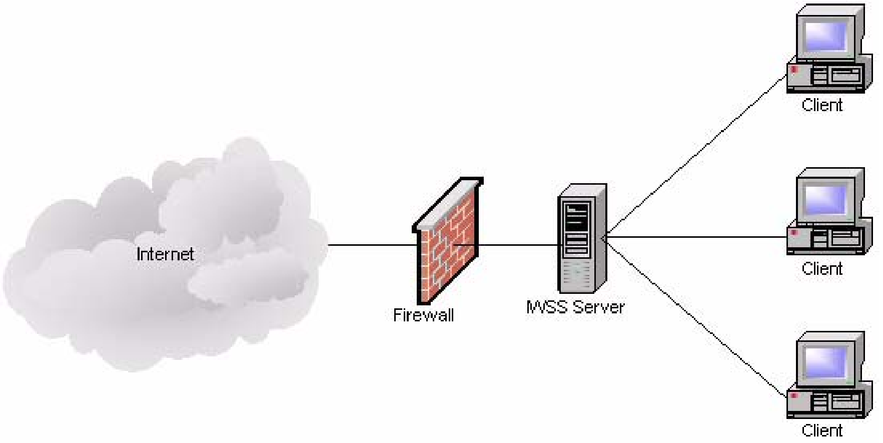


FIGURE A-5 HTTP Proxy in Standalone Mode

TABLE A-5. HTTP Proxy in Standalone Mode

Advantage	Limitation
Simple to install and manage	Slow connection reaches maximum allowed connections limit.

Stand-alone Mode with Multiple Servers

Multiple IWSS servers can be installed to balance your network traffic and scanning load. In this installation example, a Layer 4 switch receives clients requests and then forwards them to the IWSS servers.

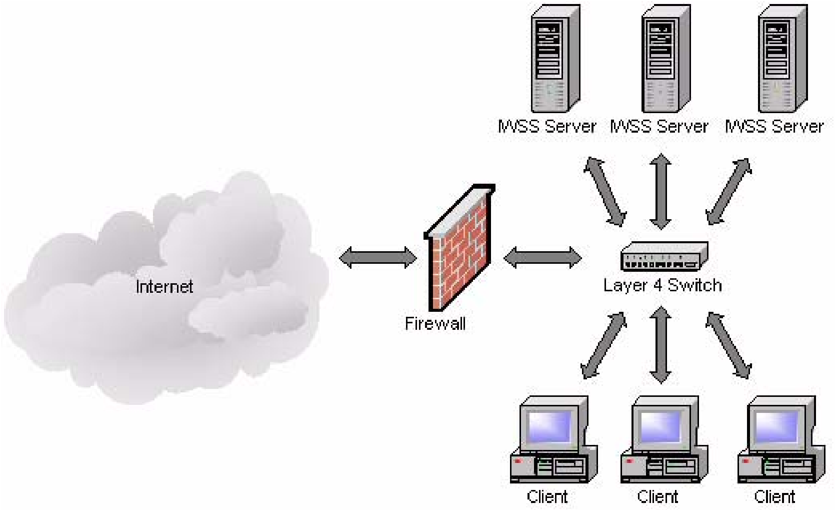


FIGURE A-6 Use a Layer 4 switch to load balance between IWSS servers for multiple HTTP stand-alone servers

HTTP Proxy in Dependent Mode (Proxy Ahead)

For HTTP browsers to use this flow, configure the browsers to proxy through the IWSS server, by default at port 8080.

Web page requests follow this sequence:

1. The Web client sends a request to the HTTP service.
2. The HTTP service validates the request.
   - If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
   - If the URL is valid, the HTTP service forwards the request to an upstream HTTP proxy server.

3. The upstream proxy server performs its processing, then forwards the request to the Web site on the Internet
4. The contacted Web site returns a response (ideally a Web page) to the HTTP proxy server.
5. The HTTP proxy server performs its processing on the returned data, then forwards the response data to the IWSS HTTP service.
6. The HTTP service scans the content for unwanted data and returns an appropriate response to the HTTP client.

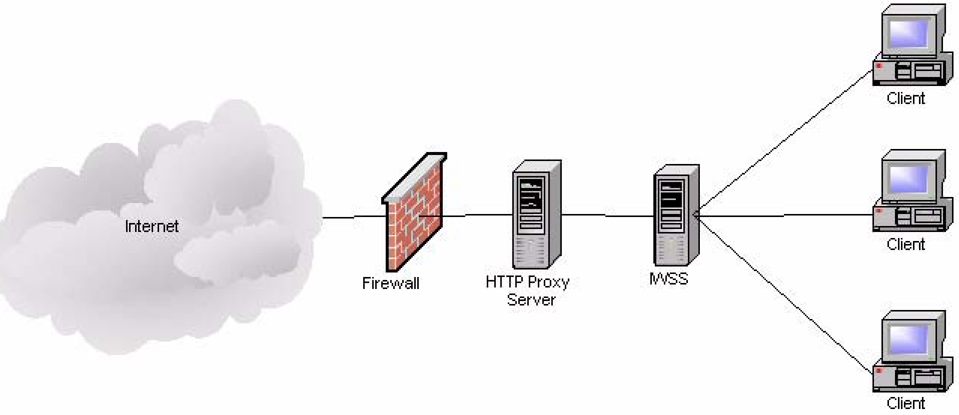


FIGURE A-7 HTTP Proxy in Dependent Mode (Proxy Ahead)

TABLE A-6. HTTP Proxy in Dependent Mode (Proxy Ahead)

Advantages	Limitations
Proxy server controls timing and content availability behavior	IWSS has to scan every response-even if cached.
It is more secure-configuration changes will affect cached objects.	
IWSS does not wait for download of already cached objects.	

HTTP Proxy in Dependent Mode (Proxy-behind)

The proxy behind flow consists of a caching proxy placed between the HTTP client and the IWSS server without using ICAP. Organizations typically use this flow to increase performance, as with ICAP.

WARNING! *Two security trade-offs exist for this potential performance enhancement:*
1. If the cache contains data with a virus, for which there was no pattern when the data hit the cache, the IWSS HTTP service is powerless to prevent the spread of the virus.
2. 2.Similarly, if a policy regarding valid content changes, or unauthorized users request data that exists in the cache (for authorized users), the HTTP service is powerless to prevent subsequent unauthorized access to this data.

Instead of using the proxy-behind flow, Trend Micro recommends that administrators use an ICAP caching device. This solution provides the performance enhancements of caching without the security issues of proxy-behind topology.

Web page requests follow this sequence:

1. The Web client sends a request to HTTP proxy server.
2. The proxy server forwards the request to IWSS.
3. IWSS validates the request using URL Filtering/Blocking.
   - If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
   - If the URL is valid, the HTTP service forwards the request to the Web server on the internet.
4. The contacted Web server returns a response (ideally a Web page) to IWSS.
5. IWSS performs its processing on the returned data (virus, spyware, ActiveX scanning), then forwards the appropriate response/data to Proxy server.
6. The Proxy server caches the data (if cacheable), then delivers the response/data to the HTTP client.

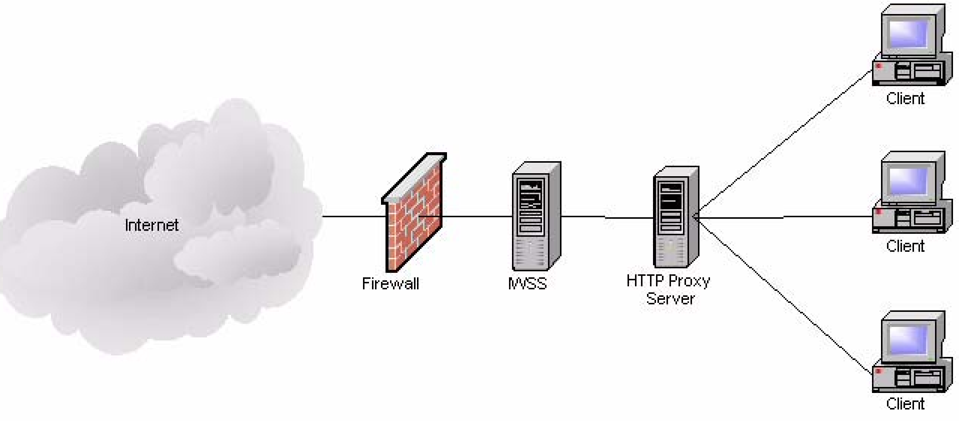


FIGURE A-8 HTTP Proxy in Dependent Mode (Proxy Behind)

TABLE A-7. HTTP Proxy in Dependent Mode (Proxy Behind)

Advantages	Limitations
No configuration changes required on the clients	Configuration changes on IWSS affect cached objects
Cached objects are downloaded by clients directly from the Proxy server, which minimizes delays	

HTTP Double Proxy in Dependent Mode

Double proxy configuration requires two caching proxies. The first proxy is placed between the HTTP client and the IWSS server, and other one is placed between the IWSS server and the Internet. This is typically used to get the advantages of the two configurations of Dependent Mode: Proxy-ahead and Proxy-behind.

Web page request follows this sequence:

1. The Web client sends a request to first proxy server.
2. The first proxy server forwards the request to IWSS.

3. IWSS validates the request using URL Filtering/Blocking.
   - If the URL is invalid (blocked) the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
   - If the URL is valid, the HTTP service forwards the request to the second proxy server.
4. The second proxy server performs its processing, then forwards the request to the Web server on the internet.
5. The contacted Web server returns a response (ideally a Web page) to second proxy server.
6. The second proxy server caches the data (if cacheable), then deliver the response/data to IWSS.
7. IWSS performs its processing on the returned data (Virus, Spyware, ActiveX scanning), then forwards the appropriate response/data to first proxy server.
8. The first proxy server caches the data (if cacheable), then delivers the response/data to the HTTP client.

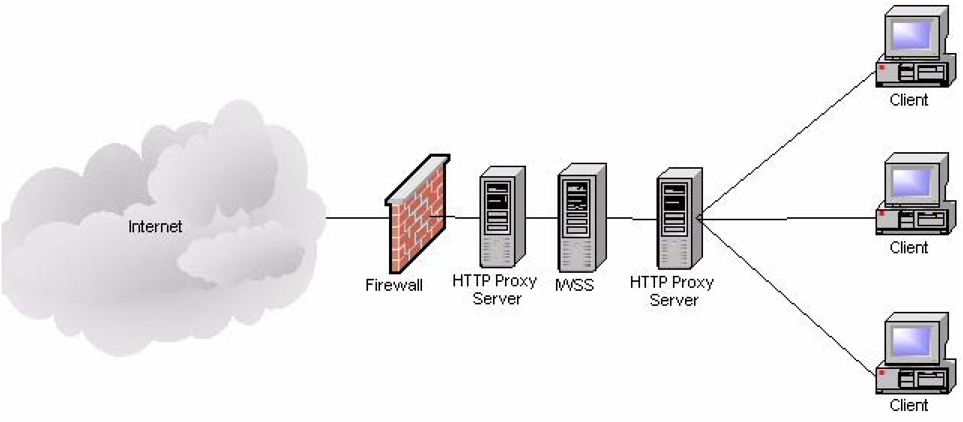


FIGURE A-9 HTTP Double Proxy in Dependent Mode

TABLE A-8. HTTP Double Proxy in Dependent Mode

Advantages	Limitations
Proxy server controls timing and content availability behavior	Costs more-- additional proxy server is needed
It is more secure-configuration changes will affect cached objects	
IWSS does not wait for download of already cached objects	
No configuration change required on the clients	

HTTP Proxy in Transparent Mode

For HTTP browsers to use this flow, no special browser configuration is required. However, the router must be specially configured to "know" where to send HTTP requests. Administrators can configure routers, which support Layer 4 port-based switching to perform this task.

Note: Transparent proxy will not work with very old browsers which do not provide host information. User identification can only rely on IP addresses when using transparent proxy as no user info is available to the IWSS server for LDAP verification.

To process HTTP requests without needing to change client Internet connection settings, IWSS supports simple transparency.

Simple Transparency

In simple transparency, clients connect to a router which redirects the requests to IWSS. FTP over HTTP connections are not available when using simple transparency. In order to integrate IWSS with DCS when using simple transparency, note the following:

- Do not use any source NAT (IP masquerade) downstream of IWSS, since IWSS needs to know the IP address of the client to clean.
- A DNS server is needed for DCS to resolve the client machine name from its IP address in order to perform a cleanup.

HTTP Reverse Proxy in Dependent Mode

In reverse proxy mode, IWSS protects a Web server with the proxy server. The HTTP proxy is placed between the Internet and the Web server. This is useful when the Web server accepts file uploads from clients, or to reduce the load of each Web server by balancing the load among multiple Web servers. ASPs/ISPs use IWSS as an HTTP proxy to protect the upload traffic against viruses, and organizations with complex Web sites need it as a centralized point of access control.

This flow is especially useful for Web sites involved in e-commerce transactions, distributed applications, which exchange data across the Internet, or other situations where clients upload files to the Web server from remote locations.

In reverse proxy mode, the HTTP proxy acts as the Web server to the client systems. The proxy receives all requests and transfers them to the real Web server. Consequently, all HTTP traffic goes through the HTTP proxy, enabling the proxy to scan to content and block any infected transactions.

Note: Administrators should be aware of the following
1. The URL-filtering feature makes no sense in this configuration; only anti-virus scanning and URL-blocking are useful.
2. In reverse proxy mode, the Web server's access log is useless. To analyze the connections for the Web site, you must use the proxy's access log.
3. Ideally, the reverse proxy server should be placed behind a firewall, but in many cases, the proxy is connected directly to the Internet, where it is more vulnerable to direct attacks. When a reverse proxy is configured without a firewall, administrators should take all appropriate precautions in securing the operating system hosting IWSS

Web page requests follow this sequence:

1. Clients initiate WebWebWeb request.
2. The request is received by InterScan Web Security Suite, configured to listen on port 80.
3. InterScan Web Security Suite scans the content, then forwards it to an actual Web server.
4. The Web server delivers the requested page back to IWSS.
5. InterScan Web Security Suite rewrites the page headers, and sends on the request.
6. The modified page returns to the requestor.

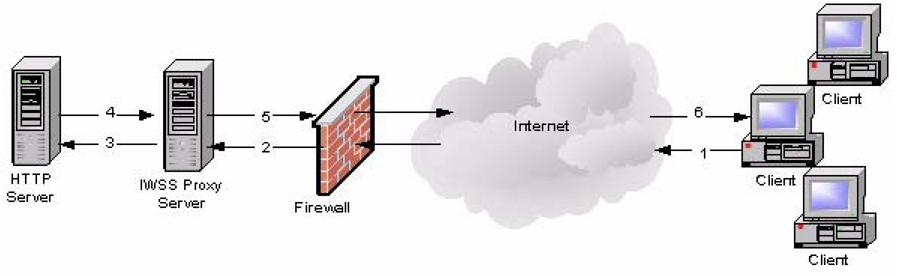


FIGURE A-10 HTTP Reverse Proxy in Dependent Mode

TABLE A-9. HTTP Reverse Proxy in Dependent Mode

Advantages	Limitations
IWSS scans all objects only once-before they are cached	New engine, pattern, and configurations will not affect cached objects.
	Access logging feature of IWSS is compromised.

HTTP Proxy in ICAP Mode (Single and Multiple IWSS Servers)

This section discusses the flow of a typical HTTP GET request using both an ICAP device and IWSS servers. In these flows, IWSS interacts with the ICAP device, in response to ICAP rules. This is very different from other flows where IWSS receives URL requests form HTTP clients. To use these flows for HTTP browsers, configure the browsers to use the ICAP device as the HTTP proxy.

Using ICAP devices can enhance performance in two ways:

- **Caching good data**–If the data is clean, the ICAP device caches the data. Subsequent requests require only four steps, not eight. (ICAP must still ask IWSS to check the policies to validate that the users making the subsequent requests can browse the data, has not exceeded his or her quota, etc.)
- **Clustered IWSS servers**—When multiple IWSS servers are used, the ICAP device load balances the requests between the servers. This is vital for enterprise

environments where the demand for scanning incoming pages can overwhelm a single IWSS server. With ICAP, the ICAP device performs load balancing, and receives maximum performance from the available IWSS servers.

Note: Non-ICAP environments can receive similar benefits by using multiple IWSS servers. However, the administrator must configure different users to proxy through the available IWSS servers and estimate how many and which clients to assign to each.

When IWSS is configured in ICAP mode, it processes requests from any ICAP-compliant client. Trend Micro supports the following ICAP client implementations:

- NetCache
- Blue Coat
- Cisco Content Engines

Although IWSS performs the same filtering of URLs and scanning of data for unwanted content, the ICAP flow is so different from the other flows that it requires a completely different communications protocol. Administrators indicate which protocol (ICAP or non-ICAP) to use during post-installation configuration.

The following figures show the HTTP flow with single and multiple IWSS servers. (Both images assume the requested data in not in the ICAP device's cache.) The ICAP service determines which IWSS server receives the request in a multi-server environment.

Web page requests follow this sequence:

1. An HTTP client makes a request for a URL, sending the request to the ICAP caching proxy device.
2. The ICAP device, based on its configuration, determines that the request must be forwarded to an IWSS server. If multiple servers are available, it alternates in round-robin fashion for load balancing.
3. The IWSS server validates the URL.
   - If the URL is not blocked, IWSS sends the response to the ICAP device.
   - If the URL is invalid (blocked), IWSS directs the ICAP device to send an appropriate response to the HTTP client and the transaction is complete.

4. If the URL is valid, the ICAP server requests the page from the Web site on the Internet.
5. The Web site on the Internet returns the requested page (or some other appropriate response).
6. If the page is returned, the ICAP device, based on its configuration, determines that an IWSS server must scan the data. Again, if multiple servers are available, it alternates in round-robin fashion for load balancing.
7. The IWSS server scans the results and returns an appropriate response to the ICAP device, based on whether the data is clean or contains unwanted content.
8. If the data is clean, the ICAP device returns said data to the HTTP client, and the ICAP device retains a copy of the data to satisfy future requests. If the data contains unwanted content, the ICAP device returns an appropriate error message (dictated by IWSS) to the HTTP client, and the ICAP device does not retain a copy for future requests.

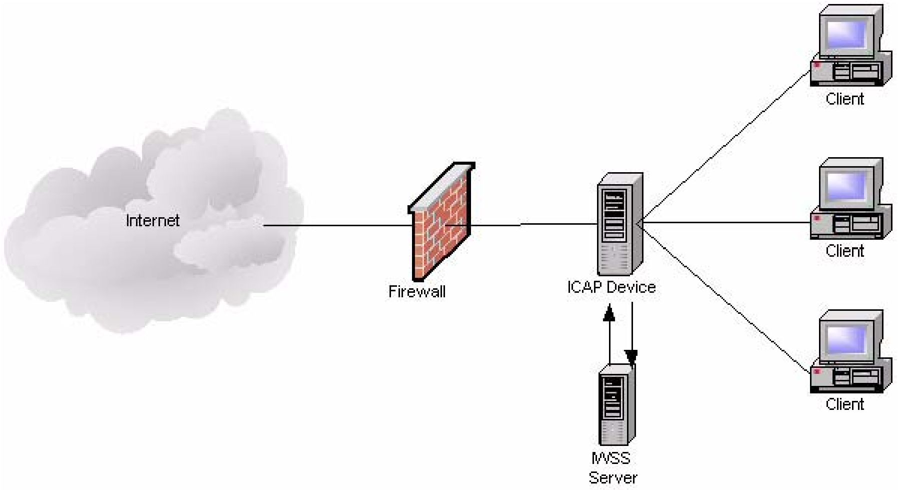


FIGURE A-11 HTTP Proxy in ICAP Mode (Single IWSS Server)

IWSS ICAP Mode with Multiple Servers

If there is already a content cache server on your network, then Trend Micro recommends installing the ICAP HTTP handler. The following diagram shows the installation topology for IWSS ICAP with multiple servers. For multiple IWSS ICAP servers to work properly, their corresponding pattern, scan engine version, and intscan.ini files must be identical, and all servers should connect to the same database.

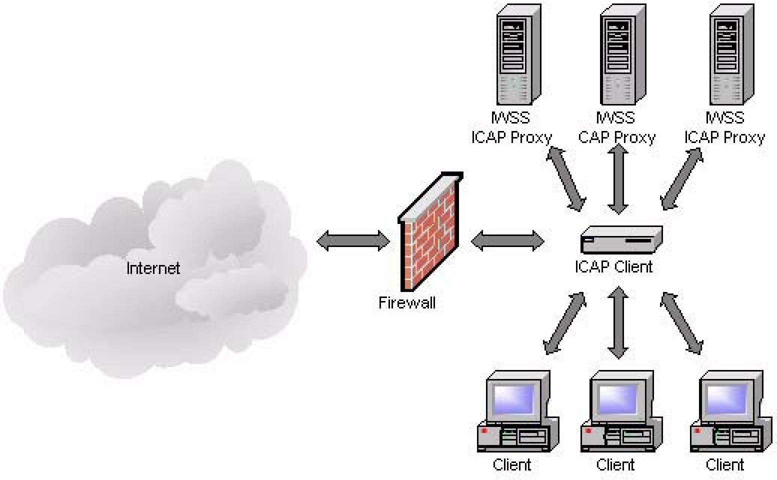


FIGURE A-12 HTTP Proxy in ICAP Mode (Multiple IWSS Servers)

TABLE A-10. HTTP Proxy in ICAP Mode

Advantages	Limitations
No configuration changes required on the clients	User identification on IWSS is not supported; thus, limited reporting
Cached objects are downloaded by clients directly from the Proxy server, which minimizes delays, and improves performance	Configuration changes on IWSS affect cached objects
Load-balancing possible after some configuration to the clients	

Planning FTP Flows

There are two possible FTP flows: standalone and dependent. They are similar to the stand-alone and dependent-mode flows for HTTP service. Each requires a different configuration and has its own implications including:

- **Stand-alone**—the IWSS server acts as an FTP proxy server between the requesting client and the remote site, brokering all transactions
- **Dependent**—IWSS works in conjunction with another FTP proxy server within a LAN

FTP Proxy in Standalone Mode

To scan all FTP traffic in and out of the LAN, set up the FTP scanning module so that it "brokers" all such connections. In this case, clients FTP to the IWSS server, supply the logon credentials to the target site, and then allow the IWSS FTP server to make the connection. The remote site transfers the files to IWSS FTP. Before delivering the files to the requesting clients, the IWSS FTP server scans the files for viruses and other security risks

The implications for the FTP standalone flow are:

- IWSS must have access to the target FTP servers
- There is one less step in the flow, compared to the FTP proxy mode

To configure FTP clients to use this flow:

- Set the IWSS server as a FTP proxy
- Set the user name to be `username@targetftp-server`, instead of the normal username

Note: IWSS FTP works with most firewalls, usually requiring only a modification to the firewall to open a port for the FTP proxy.

FTP requests follow this sequence:

1. The FTP client sends a request to the IWSS FTP service.
2. The IWSS FTP service validates the request (for example, the file type is not blocked). If the request is valid, the IWSS FTP service attempts to connect to the appropriate FTP server on the Internet. If the connection succeeds, the IWSS FTP service sends the request to the target FTP server.

3. The FTP server on the Internet responds to the request, ideally with the requested file.
4. The IWSS FTP service scans the returned data for unwanted content. If it finds any unwanted content, it returns an appropriate message to the FTP client. Otherwise, it returns the requested data to the FTP client.

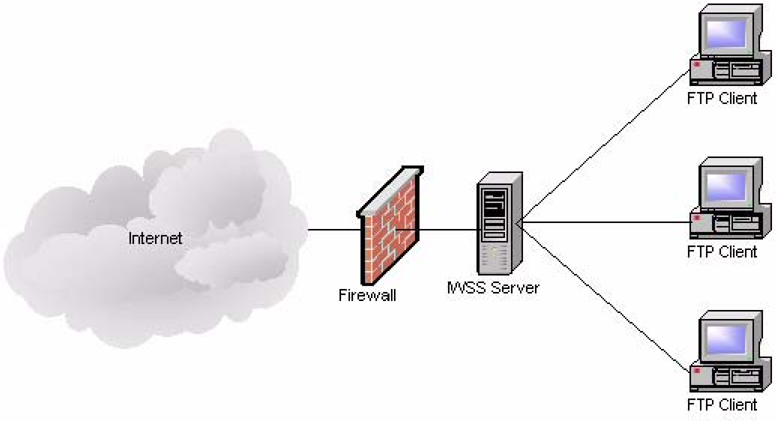


FIGURE A-13 FTP Proxy in Standalone Mode

FTP Proxy in Dependent Mode

You can also install IWSS FTP on a dedicated machine between an upstream proxy and the requesting clients. Use this setup adds other FTP features (for example, access blocking, logging, and filtering) to supplement the existing FTP proxy.

IWSS's FTP-proxy mode, shown in Figure A-14, is analogous to the dependent-mode flow of the HTTP service. Because it carries a performance penalty of an extra hop and extra processing by the other FTP proxy server, only use this mode if your organization does not allow the IWSS Server to access the Internet directly.

If the other FTP proxy server uses a store-and-forward technique, the performance penalty is more noticeable on large files because the other FTP proxy first downloads the file and passes it on to the IWSS FTP service. Additionally, the other FTP proxy must have sufficient free disk space to hold all transfers in progress.

Unlike the HTTP dependent-mode service, which has the possible benefit of cached requests, most FTP proxy servers do not cache requests.

FTP Dependent Mode also protects FTP servers from upload and download threats.

FTP requests follow this sequence:

1. The FTP client sends a request to the IWSS FTP service.
2. The IWSS FTP service validates the request (for example, the file type is not blocked). If the request is valid, the IWSS FTP service relays it to the other FTP proxy or the FTP server being protected by IWSS.
3. The FTP server on the Internet responds to the request, ideally with the requested file.
4. The IWSS FTP service scans the returned data for unwanted content. If it finds any unwanted content, it returns an appropriate message to the FTP client. Otherwise, it returns the requested data to the FTP client.

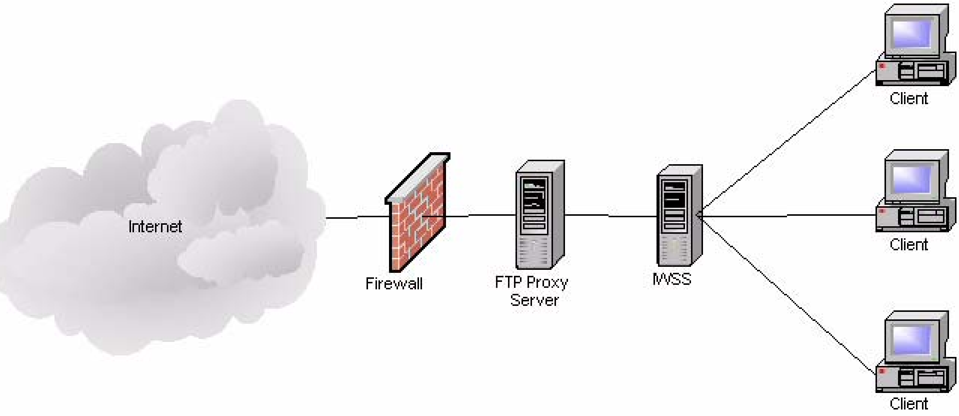


FIGURE A-14 FTP Proxy in Dependent Mode

Component Planning

Note: Trend Micro recommends installing IWSS on a dedicated server.

Select the components to install:

- **Main Program**—installs the management console and the basic library files necessary for IWSS.
- **HTTP Scanning**—installs the service necessary for HTTP scanning (either ICAP or HTTP proxy) and URL blocking.
- **FTP Scanning**—installs the service necessary for FTP scanning.
- **URL Filtering**—installs the service necessary for URL filtering (not enabled by default). Requires a separate Activation Code.
- **Applets and ActiveX Scanning**—installs the service necessary for scanning Java applets and ActiveX controls. Requires a separate Activation Code.
- **IntelliTunnel Security**—installs the service necessary to block communication provided by certain Instant Message (IM) protocols and certain authentication connection protocols.
- **SNMP Notifications**—installs the service to send SNMP traps to SNMP-compliant network management software.
- **Control Manager Agent for IWSS**—installs the files necessary for the Control Manager agent. You need to install the agent if you are using Control Manager (Trend Micro's central management console).

Note: URL Filtering and Applets and ActiveX Scanning each require a separate Activation Code.

Staging a Pilot Deployment

Before performing a full-scale deployment, Trend Micro recommends that you first conduct a pilot deployment in a controlled environment. A pilot deployment provides an opportunity to determine how features work and the level of support you will need after full deployment.

It also gives your installation team a chance to rehearse and refine the deployment process and discover if your deployment plan meets your organization's security needs.

Note: Although this phase is optional, Trend Micro highly recommends conducting a pilot deployment before doing a full-scale deployment.

Choosing a Test Environment

Choose a test environment that matches your production environment. Try to simulate the type of network topology that would serve as an adequate representation of your production environment.

Creating a Rollback Plan

Trend Micro recommends creating a disaster recovery or rollback plan in case there are issues with your installation or upgrade process

Deploying Your Pilot

Evaluate the different methods of deployment (See *Planning HTTP and FTP Service Flows* on page A-14) to see which ones are suitable for your environment.

Evaluating Your Pilot Deployment

Create a list of successes and failures encountered throughout the pilot process. Identify potential pitfalls and plan according for a successful deployment. This pilot evaluation plan can be rolled into the overall production plan.

Appendix B

Deployment Integration

This appendix introduces InterScan Web Security Suite, and describes the main considerations before installing the software in your environment.

Topics in this chapter include:

- *IWSS in a Distributed Environment* starting on page B-2
- *Connection Requirements and Properties* starting on page B-2
- *Integration with LDAP* starting on page B-3
- *Damage Cleanup Services (DCS) Integration* starting on page B-5
- *Integration with Cisco Router* starting on page B-7

IWSS in a Distributed Environment

IWSS is designed to be part of a distributed system and can establish a number of network connections based on the configuration settings.

The administrator must ensure the following:

- None of the required channels are blocked
- All channels have enough throughput
- Servers use a supported version of the software
- Servers have enough performance

Connection Requirements and Properties

Table 2-1 below gives the required connections and their properties.

TABLE 2-1. Required Connections and Properties

Connecting Component	Traffic: Type and Volume	If the Connection is lost
Clients	Should be measured on the real network	No protection
Database server	**Type:** TCP **Volume:** • **Low**—if access logging is disabled • **Medium**—if access logging is enabled	Cached data is used for already started services. Services will not start.
LDAP server (if configured)	**Type:** LDAP **Volume:** Medium	Cached data is used for already started services. Services will not start.
Trend Micro Active Update Server	**Type:** HTTP and HTTPS **Volume:** 10-50 Mb/day	IWSS components cannot be updated in time.
Trend Micro Dynamic Categorization server (if configured)	**Type:** HTTP **Volume:** Depends on the specific access	Requested resources are not categorized properly. URLs prohibited by policy settings can be accessible.

TABLE 2-1. Required Connections and Properties (Continued)

Connecting Component	Traffic: Type and Volume	If the Connection is lost
Trend Micro DCS server (if configured)	**Type:** HTTP **Volume:** Depends on the number of infected machines	No cleaning is performed for infected machines.

Throughput and Availability Requirements

The administrator must determine the IWSS availability requirements.

- Is IWSS downtime acceptable?
- If so, what is the proper action (bypass or stop) to enforce when IWSS is down?
- If a failover configuration with multiple IWSS instances is used, do the LDAP server and the database server have the same level of failover?

Integration with LDAP

Support Referral Chasing for Multiple LDAP Servers

IWSS has an LDAP module that allows communication with multiple LDAP servers with the ability to establish multi-domain tree- and forest-like environments.

If the configured main LDAP server from the IWSS Web console **HTTP > Configuration > User Identification** page cannot resolve client credentials, and the “referral chasing” is enabled (providing that the referral server(s) is configured), IWSS attempts to query for the requested User/Group object with the configured Primary Referral Server. If the queried object is still not found, a configured Secondary Referral will be queried. In order to do that, it must keep the credentials of the administrative account for all LDAP servers in the `[LDAP-Setting]` section of the intscan.ini file.

Global Catalog

The Windows Active Directory (AD) Global Catalog enables LDAP clients, such as IWSS, to query objects native to the domain being queried, and those residing in remote domains, as long as the AD server being queried and the remote AD server has Global Catalog enabled. The Global Catalog server accepts the LDAP requests on port 3268 and allows querying the user credentials, full name and membership in the global and universal groups across all other domains in the forest. The use of the Global Catalog is handy when creating IWSS LDAP policies for a parent group with user(s)/group(s) member(s) residing on remote domains that are part of many sub-domain levels.

To use this feature, the IWSS administrator should configure the main LDAP server that IWSS uses from the Web console **HTTP > Configuration > User Identification** page to communicate with a designated Global Catalog-enabled Active Directory server using port 3268, instead of using the default LDAP communication port 389.

Note: Global Catalog is available only in Microsoft Active Directory. The advantage of using the Global Catalog port includes better performance for LDAP object lookup, and allows object lookup that resides in many sub-levels of the Active Directory tree (beyond three). However, in order for IWSS to utilize the Global Catalog, the AD being requested for an object needs to have the Global Catalog enabled along with the AD where the queried user/group object reside. IWSS supports the use of the Global Catalog port only to be configured as the main LDAP server, and not part of the IWSS referral chasing servers.

Guest Account

When LDAP support is enabled, IWSS works in the authenticated proxy mode. It requires authentication for every client. This rule can cause problems for guest/mobile computers, whose users are not registered in the local LDAP server.

To resolve this issue, the HTTP scanning service in the HTTP proxy mode supports an additional listening point that can be used as a proxy server specification for the guest computers.

The following configuration parameters control this behavior:

- `intscan.ini/[http]/guest_user_login` enable guest port
- `IWSSPIProtocolHttpProxy.pni/[main]/guestport`port number on which to listen

IWSS bypasses the LDAP-based user identification and applies the special (Guest) policies to every computer accessing it over this port.

Damage Cleanup Services (DCS) Integration

While IWSS can detect and block worms and spyware at the HTTP and FTP gateway, it can also work in conjunction with Trend Micro Damage Cleanup Services to clean infected clients. Damage Cleanup Services is a comprehensive service that helps assess and clean system damage without installing software on client computers in a network. It performs the following activities:

- Removes registry entries created by worms and Trojans
- Removes memory resident worms, Trojans, and spyware/grayware
- Repairs system file configurations modified by malware

After IWSS is registered with one or more DCS servers, IWSS issues a cleanup request if it detects one of the following trigger conditions:

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

Note: If malware attempts to contact a remote server using a protocol other than HTTP, IWSS will not detect it, thus will not trigger a cleanup.

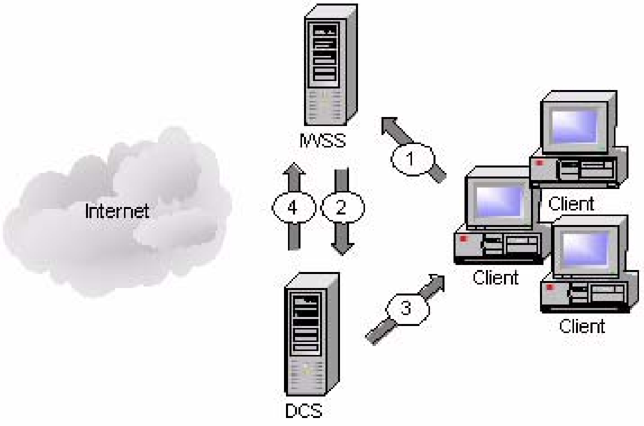


FIGURE B-1 How IWSS requests DCS to perform a client cleanup

When IWSS registers to a DCS server, infected client cleanups are handled in the following manner:

1. IWSS detects the client attempting to access a URL listed in the PhishTrap pattern file or upload a worm.
2. IWSS requests the DCS server to clean up the infected client.
3. DCS attempts to connect to the infected client and clean it through remote procedures.
4. DCS reports the outcome of its cleaning attempt to IWSS for logging.

When it receives a cleanup request from IWSS, DCS attempts to connect to the infected client and repair the system damage. The outcome of the cleaning attempt, either successful or unsuccessful, is reported back to the IWSS server for logging. If the cleanup attempt is not successful, then the client is redirected to a Web page hosted on the DCS server and an ActiveX control again attempts to clean the infected computer, with the permission of the computer's user.

Note: If you are using DCS in conjunction with a HTTPS-enabled IWSS Web management console, IWSS must be configured to allow access to the secure port (typically 8443). If access to the secure port is blocked, IWSS will be unable to redirect clients to DCS for clean-up requests. For more information, see *Using SSL with Damage Cleanup Services (DCS)* starting on page 5-21.

Integration with Cisco Router

You can integrate IWSS on a network that uses a Cisco router at the gateway without changing the browser settings of the client machines.

To resolve the issue, integrate IWSS on the network through transparent proxy configuration by setting up the Policy-based Routing (PBR) on the Cisco router with the following policies:

Policy 1 Conditions:

- If the packet is from the IWSS server
- If the packet is for port 80/tcp and/or 443/tcp

Action: Routes the packet to the Internet.

Policy 2 Conditions:

- If the packet is from the local area network (other than the IWSS server)
- If the packet is for port 80/tcp and/or 443/tcp
- If the packet is not from the IWSS server

Action: Forwards the packet to the IWSS proxy port

For information on configuring policy-based routing, refer to the *Cisco Online Configuration Guide*.

Note: In IWSS 3.0, set IWSS to transparent proxy when implementing this setup. For additional information, see *Using an ICAP-enabled Proxy* starting on page A-12.

Appendix C

Tuning and Troubleshooting

This chapter provides information to optimize your IWSS installation's performance tuning and installation troubleshooting.

Topics in this chapter include:

IWSS Performance Tuning

If you are experiencing issues with slow browsing performance, consider the following modifications and the IWSS remote rating service.

URL Filtering

IWSS uses a two-tier lookup system for categorizing URLs. Primarily, IWSS relies on a local database of URLs and ratings, and all requests are first checked against this pattern. This pattern is regularly updated by Trend Micro. Since the database can be quite large, and takes significant processing power to import, Trend Micro recommends scheduling URL filtering database updates during non-work hours.

Secondarily, IWSS can connect to Trend Micro's remote rating service (RS) (via HTTP) to request categorization for any URL that meets the following criteria:

- The URL cannot be categorized by the local URL database.
- The host of the URL is not in IP format in the range of private class A, B, or C network addresses.
- The URL does not appear in the "URL Filtering Exceptions" list.

The RS uses its own copy of the URL database which is nearly identical in content to the pattern used locally by IWSS, but the RS pattern is continuously updated. If the URL that IWSS needs to categorize is in the delta of URLs that have been rated since the last time IWSS performed a URL database update, then the RS will be able to provide the rating. If not, the RS will flag that URL for future rating by Trend Micro technicians.

Since the RS relies on an additional HTTP transaction, it can introduce significant latency into certain environments. IWSS uses a cache to reduce the amount of necessary RS transactions, but networks with very diverse traffic may still experience a slowdown when the RS is enabled.

The RS is enabled by default. To disable it, manually edit the `urlfcIfx.ini` file located in the IWSS install directory. Set the value of the parameter `[network]/no_web_access` to "yes" and restart the IWSS HTTP service.

LDAP Performance Tuning

When running IWSS to use the user/group name via proxy authorization identification method (LDAP), HTTP proxy performance becomes dependent upon the responsiveness of the LDAP directory server. In a worst case scenario, every HTTP request would require an LDAP query to authenticate the user's credentials, and another to retrieve group membership information for that user. These queries introduce latency in terms of the transmit/receive delay between IWSS and the LDAP server, and add load to the LDAP server itself.

LDAP Internal Caches

To reduce the amount of LDAP queries required, IWSS provides several internal caches:

- User group membership cache: This cache can store the group membership information for several hundred users. By default, entries in this cache will be valid for 48 hours, or until the cache fills (at which point entries are replaced, starting with the oldest). The time to live (TTL) for entries in this cache can be configured via the setting “user_groups_central_cache_interval” in the [user-identification] section of intscan.ini configuration file.
- Client IP to User ID cache: This cache associates a client IP address with a user who recently authenticated from that same IP address. Any request originating from the same IP address as a previously authenticated request will be attributed to that user, provided the new request is issued within a configurable window of time (15 minutes by default for HTTP, 90 minutes for ICAP) from that authentication. The caveat is that client IP addresses seen by IWSS must be unique to a user within that time period, thus this cache is not useful in environments where there is a proxy server or source NAT between the clients and IWSS, or where DHCP frequently reassigns client IPs. To enable or disable this cache, change the “enable_ip_user_cache” setting in the [user-identification] section of intscan.ini. To change the TTL of this cache, change the “ip_user_central_cache_interval” (unit is hours). For example, to create a TTL of 30 minutes, then enter “0.5”.
- User authentication cache: This avoids re-authenticating multiple HTTP requests passed over a persistent connection. When users pass the credential validation over a persistent connection, IWSS adds an entry (two important keys in one cache entry are the client’s IP address and the client’s username) in the user authentication cache so the subsequent requests over a keep-alive connection will

not authenticate again. The client IP address and client’s username serve as two forward references, or links, to the “client IP to user ID cache” and “user group membership cache,” respectively. IWSS will thus still be able to retrieve the user’s connection information from both the IP-user and user-group caches.

When deploying IWSS with LDAP integration, it is important to consider the additional load that authenticating HTTP requests will place on the LDAP directory server. In an environment that cannot effectively use the client IP to user ID cache, the directory server will need to be able to handle queries at the same rate as IWSS receives HTTP requests.

Disable Verbose Logging When LDAP Enabled

Trend Micro recommends turning off verbose logging in the intscan.ini file, under the [http] section, “verbose” parameter) when LDAP is enabled for server performance reasons. Verbose logging is primarily used by software developers to identify abnormal application behavior and troubleshooting. In a production deployment, verbose logging is usually unnecessary.

If verbose logging is enabled and LDAP is also enabled, IWSS will log user authentication information and group membership information in the HTTP log in the \Log folder. Logs may contain hundreds of lines per user and therefore significantly consume disk space, depending on the amount of internal traffic and the number of groups a user is associated with. Verbose logging keeps the service busy with issuing I/O operations to the operating system. This may prevent the service from responding to HTTP requests in a timely fashion, hence latency may occur. In an extreme bursting HTTP traffic environment, it’s possible to observe significant delays when IWSS starts up in verbose mode.

Troubleshooting

Troubleshooting Tips

- **Issue:** IWSS could not connect to the database specified in the Database Connection Settings page. The IWSS management console displays the following error message:

  ```
  JDBC-ODBC BRIDGE: [unixODBC]Could not connect to the server;
  Could not connect to remote socket.
  ```

Solution:

- Please check the ODBC connection and/or database server and try again.

- **Issue:** The IWSS management console displays an authentication error message.

```
JDBC-ODBC BRIDGE: [unixODBC]FATAL: Password authentication
failed for user.
```

Solution:

- Verify the user credential for the PostgreSQL Server and also ensure that the database settings are correct (**Administration > IWSS Configuration > Database | Database Setting**). If the problem persists, ensure that the permissions in the `etc/iscan/odbc.ini` file are correct.

Before Contacting Technical Support

When contacting Technical Support with your issues, having specific information can streamline the process:

Installation Problem

Collect the following information about your installation problem before contacting Trend Micro technical support to expedite the process.

1. IWSS version and build number
2. Screenshot of the exact error that appears during installation
3. The stage of the installation / un-installation where the problem occurs
4. The `/etc/iscan/log/install.log` installation log file

General Feature Problem

If you have problems with IWSS, collect the following information to give to Trend Micro support:

1. The system file(s) that describes the current state of IWSS.

   To compile these files, access the Web console and choose **Administration > Support** and then click **Generate System Information File**. This button is an extension of the case diagnostic tool (CDT), allowing you to package the current machine “state” at a click of a button.

The system file(s) that IWSS generates from clicking the **Generate System Information File** button are packaged into a single file with the following format:

`Info_YYYYMMDD_999999.tar.tz`

Where `YYYY` is the current year, `MM` is the current month, and `DD` is the current day that the package file was generated. `999999` is the Unix time code.

The system file(s) contains the following information:

- **IWSS information**—Includes IWSS product version, engine version and build number, current pattern file (if available), and IWSS hot fixes and service pack information. Product and integration settings are also part of this information
- **IWSS/system logs**—Includes IWSS logs and debug logs, logs generated by syslogd daemon (if system logs are enabled), and core dump file
- **System/network information**—Includes the hardware configuration, operating system, build, system resource status, other application installed, and network information
- **CDT-compliant configuration/plug-ins information**—Includes information about changes made to CDT as a result of IWSS adding a new component, such as a TMCM or MCP agent.

2. Core files are first created in the first directory listed below, and then moved to the second directory listed:

- /etc/iscan/iwss/
- /etc/iscan/iwss/UserDumps

Use these files when working with Trend Micro technical support to help diagnose the cause of your problem. To view the files yourself, use a program like GDB, the GNU Project debugger.

3. Log file for the day the issue occurred

- All log files the day the issue occurred (logs are stored in `/etc/iscan/log` by default)
- Make sure `verbose=1` is set in the [ftp], [http], and [notification] sections of the `intscan.ini` file
- Make sure `log_trans=yes` is set under the [ftp] and [http] sections of the `intscan.ini` file

4. From the Web console, take a screenshot of the Summary > Scanning tab page.
5. Record the IWSS version number.
6. URL samples (if applicable)
7. Get a packet capture of the failing transaction using ethereal or tcpdump (if possible)

Additional IWSS Testing

In addition to running the EICAR test virus, you can further verify the IWSS installation by testing the following features:

- Upload scanning
- FTP scanning
- URL blocking
- Download scanning
- URL filtering
- Spyware scanning
- PhishTrap scanning
- Applet and ActiveX scanning
- IntelliTunnel Blocking

Testing Upload Scanning

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

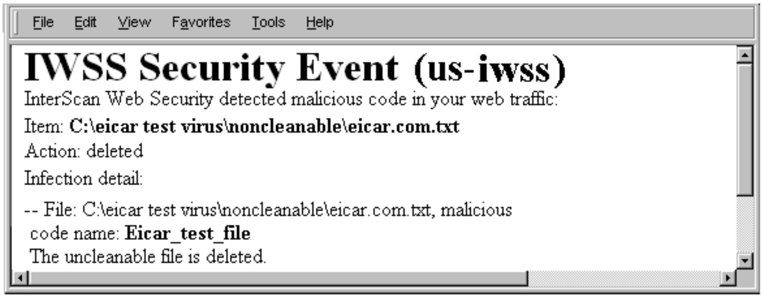
To test virus scanning of Web-based mail attachments:

1. Open the IWSS console and click **HTTP > Scan Policies** in the main menu. Clear **Enable virus scanning**, and then click **Save**.

2. Download the test virus from the following page:

   `http://www.eicar.org/anti_virus_test_file.htm`

3. Save the test virus on your local machine.
4. Re-open the IWSS console, under **HTTP > Scan Policies** in the main menu, select **Enable virus scanning**, and then click **Save**.
5. Send a message with one of the test viruses as an attachment by using any Internet mail service. A message similar to the following should display in your browser.



IWSS Security Event (us-iwss)

InterScan Web Security detected malicious code in your web traffic:

Item: **C:\eicar test virus\noncleanable\eicar.com.txt**

Action: deleted

Infection detail:

-- File: C:\eicar test virus\noncleanable\eicar.com.txt, malicious code name: **Eicar_test_file**
The uncleanable file is deleted.

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

Testing FTP Scanning

The following procedure contains instructions to test FTP virus scanning in stand-alone mode.

To test virus scanning of FTP traffic:

1. Download the test virus from the following page:

   `http://www.eicar.org/anti_virus_test_file.htm`

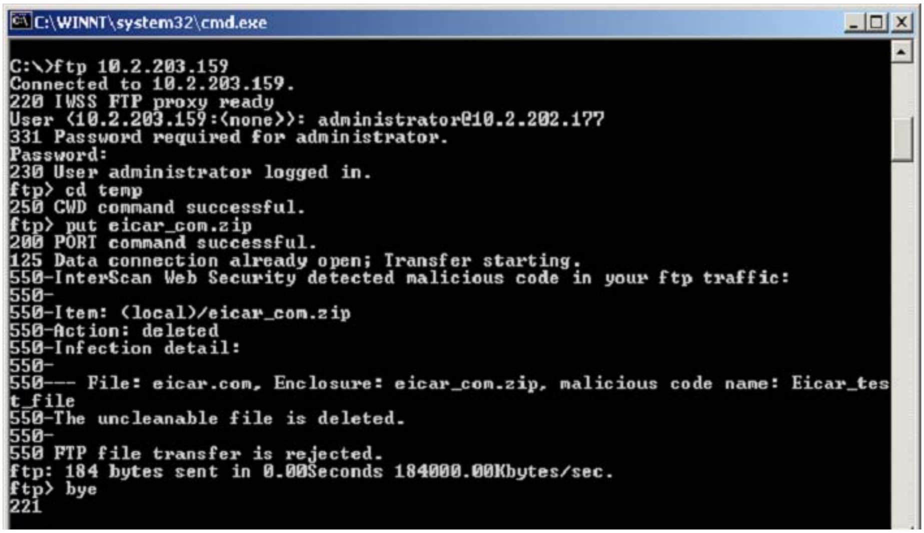
2. Access the FTP server through IWSS working as the FTP proxy.
   For example, assume the following IP addresses: IWSS FTP proxy server (`10.2.10.2`), FTP server (`10.2.10.10`).
   Open a command line prompt and type the following:

```
ftp 10.2.10.2
```

3. Log on as `user@host.` For example, if your FTP account name is `anonymous` and the IP address of the FTP server is `10.2.10.10`; then, log on as `anonymous@10.2.10.10`
4. Upload the test virus (for example, eicar_com.zip) by typing the command

   ```
   put eicar_com.zip
   ```

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



```
C:\>ftp 10.2.203.159
Connected to 10.2.203.159.
220 IWSS FTP proxy ready
User (10.2.203.159:(none)): administrator@10.2.202.177
331 Password required for administrator.
Password:
230 User administrator logged in.
ftp> cd temp
250 CWD command successful.
ftp> put eicar_com.zip
200 PORT command successful.
125 Data connection already open; Transfer starting.
550-InterScan Web Security detected malicious code in your ftp traffic:
550-
550-Item: (local)/eicar_com.zip
550-Action: deleted
550-Infection detail:
550-
550--- File: eicar.com, Enclosure: eicar_com.zip, malicious code name: Eicar_tes
t_file
550-The uncleanable file is deleted.
550-
550 FTP file transfer is rejected.
ftp: 184 bytes sent in 0.00Seconds 184000.00Kbytes/sec.
ftp> bye
221
```

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

Testing URL Blocking

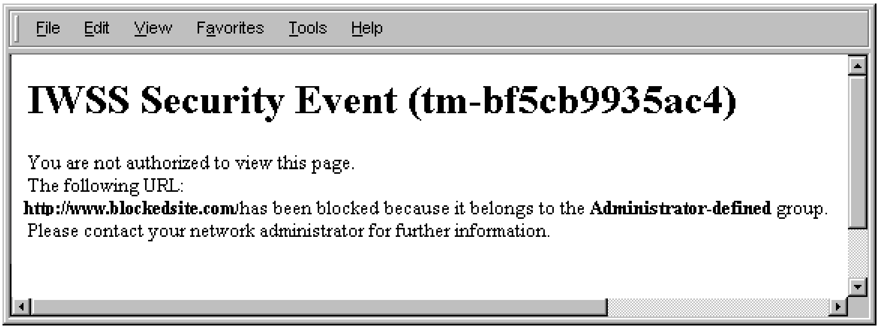
Before testing URL blocking, require your users to set the Web client's HTTP proxy to point to IWSS.

- For stand-alone mode, set the Web client's HTTP proxy to point to IWSS (for example, open Internet Explorer and click **Tools > Internet Options > Connections > LAN Settings > Use a proxy server**).

- For upstream proxy, set the Web client's HTTP proxy to point to IWSS (for example, open Internet Explorer and click **Tools** > **Internet Options** > **Connections** > **LAN Settings** > **Use a proxy server**). Open the IWSS console and click **HTTP** > **Configuration** > **Proxy Scan** in the left menu and enable **Dependent mode**. Type the proxy address and the port number.

To test URL blocking:

1. Open the IWSS console and click **HTTP** > **URL Access Control** > **URL Blocking** in the main menu and select **Enable URL blocking**.
2. In the **Match** field, type the full Web address, URL keyword, or exact-match string.
3. Click **Block**, and then click **Save**.
4. Open a Web browser and try to access the blocked Web site, a URL containing the string, or the exact-match string. A message similar to the following displays in the browser.



IWSS Security Event (tm-bf5cb9935ac4)

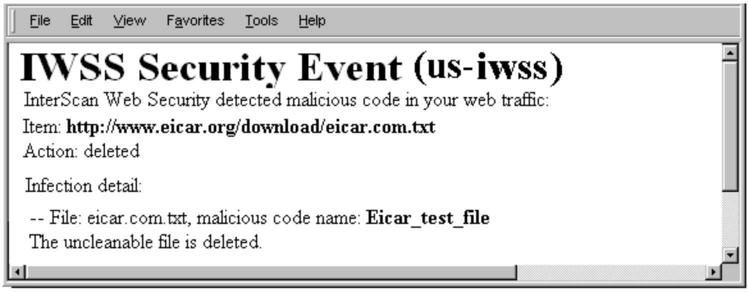
You are not authorized to view this page.
The following URL:
http://www.blockedsite.com/has been blocked because it belongs to the **Administrator-defined** group.
Please contact your network administrator for further information.

FIGURE D-3 A sample warning message for a blocked URL site.

Testing Download Scanning

To test virus scanning when downloading using HTTP or FTP over HTTP, attempt to download the test virus from the following Web site:

`http://www.eicar.org/anti_virus_test_file.htm`



IWSS Security Event (us-iwss)

InterScan Web Security detected malicious code in your web traffic:

Item: **http://www.eicar.org/download/eicar.com.txt**

Action: deleted

Infection detail:

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

FIGURE D-4 The above virus-warning screen displays if the system is set up properly.

If a client attempts to download an infected file, IWSS blocks other clients' access to that site for four hours by default. When other clients subsequently attempt to access the same URL that contained the virus, the user will see a URL blocking message instead of the virus-warning message.

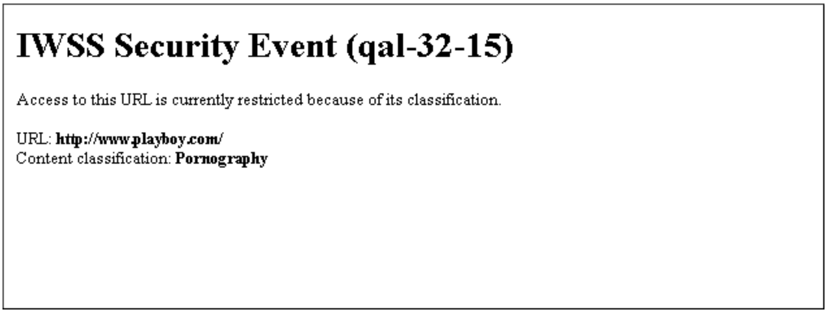
Configure the default block time (in hours) by changing the parameter `infected_url_block_length` under the `[Scan-configuration]` section of the `intscan.ini` file.

Testing URL Filtering

Trend Micro recommends that you use the default setting to test URL filtering.

To test URL Filtering:

1. Click **HTTP > URL Filtering > Settings**.
2. From the **Approved URL List** tab, review the Web site categories that are classified as "Approved URL List."
3. From the main menu, click **HTTP > URL Filtering > Policies**.
4. Select **Enable URL filtering** and then click **Save**.
5. Click **URL Filtering Global Policy** and verify that the appropriate categories are blocked during work and leisure time.
6. Open a browser and access any site (for this example, `www.urlfilteredsite.com`), which is specified in a prohibited category.



IWSS Security Event (qal-32-15)

Access to this URL is currently restricted because of its classification.

URL: **http://www.playboy.com/**
Content classification: **Pornography**

FIGURE D-5 The following message appears if the URL filtering is set up properly.

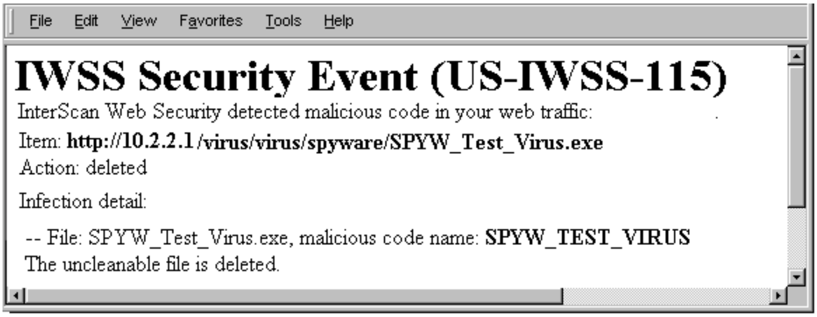
Testing Spyware Scanning

Perform the following procedure to test for spyware scanning.

To test Spyware scanning:

1. Open the IWSS console and click **Summary**.
2. Click the **Scanning** tab.
3. Enable spyware and other grayware categories for scanning by clicking **HTTP scanning**.
4. Click **HTTP > Scan Policy.**
5. Click the **Spyware/Grayware** tab and select the types of spyware/grayware which should be scanned.
6. Click the **Action** tab.
7. Under the **Uncleanable files** field, select the action setting (Delete, Quarantine, or Pass).

8. Click **Save**.
9. After a successful spyware detection, a sample message appears:



IWSS Security Event (US-IWSS-115)

InterScan Web Security detected malicious code in your web traffic:

Item: **http://10.2.2.1/virus/virus/spyware/SPYW_Test_Virus.exe**

Action: deleted

Infection detail:

-- File: SPYW_Test_Virus.exe, malicious code name: **SPYW_TEST_VIRUS**
The uncleanable file is deleted.

FIGURE D-6 A sample message after detecting a spyware with action "Delete" setting.

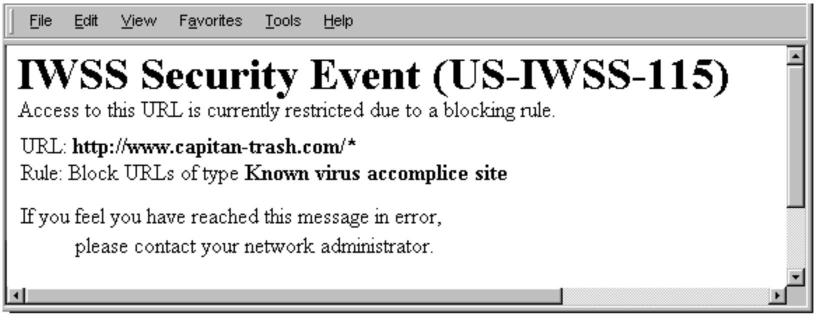
Testing PhishTrap

Perform the following procedure to test PhishTrap.

To test Phishtrap scanning:

1. Open the IWSS console and click **HTTP > URL Access Control > URL Blocking.**
2. Select **Enable URL blocking**.
3. Click the **Via Pattern File (PhishTrap)** tab.
4. Under **Block the following PhishTrap categories**, select all four categories (Phishing, Spyware, Virus accomplice, Disease vector).
5. Click **Save**.

6. After a successful phishing site detection, a sample message appears:



IWSS Security Event (US-IWSS-115)

Access to this URL is currently restricted due to a blocking rule.

URL: **http://www.capitan-trash.com/***
Rule: Block URLs of type **Known virus accomplice site**

If you feel you have reached this message in error,
please contact your network administrator.

FIGURE D-7 A sample message after detecting a phishing site.

Testing Java Applet and ActiveX Scanning

Java applets and ActiveX controls are used on many Web pages to display interactive content or applications. One way to test your installation is to temporarily configure the global policy to block all applets and ActiveX controls, and then attempt to open Web pages that use them (to verify that the applet or object is blocked).

To test Java applet and ActiveX scanning:

1. Click **HTTP > Applets and ActiveX > Policies** from the main menu.
2. If necessary, select **Enable Applet/ActiveX security** and click **Save**.
3. Click **Applet/ActiveX Security Global Policy**.
4. On the **Java Applet Security Rules** tab, click **Block all Java applets** and click **Save**.
5. On the **ActiveX Security Rules** tab, click **Block all cabinet files** and **Block all PE format files** and click **Save**.
6. Open a Web browser and attempt to navigate to Web sites that use Java applets and ActiveX controls, for example, for stock price tickers or games. IWSS will block the mobile code from downloading and running in your browser.

Note: Blocking all Java applets and ActiveX controls may be too restrictive for your environment since it will prevent many legitimate Web sites from functioning properly. After testing, Trend Micro recommends going back to the **Applets and**

ActiveX Policy: Edit Global Policy screen to change the settings back to the default or your own less-restrictive configuration.

Testing IntelliTunnel Security

To test IntelliTunnel security:

1. Download the latest MSN Messenger from `http://get.live.com/messenger/overview`
2. Install MSN Messenger.
3. Enable IntelliTunnel in IWSS.
    - **a.** Click **HTTP > IntelliTunnel**.
    - **b.** Create a new policy or open an existing one.
    - **c.** Select **MSN Messenger**.
    - **d.** Click **Save**.
    - **e.** Select the policy and then click **Deploy Policies**.
4. Configure proxy settings in Internet Explorer.
    - **a.** Open Internet Explorer.
    - **b.** Click **Tools > Internet Options**.
    - **c.** Click the **Connections** tab.
    - **d.** Click **LAN Settings**.
    - **e.** Select **Use a proxy for your LAN**. These settings will not apply to dial-up or VPN connections.
    - **f.** Enter the IWSS IP address in the **Address** field.
    - **g.** Enter the IWSS HTTP listening port in the **Port** field. This value must match **HTTP > Configuration > Proxy Scan Settings > HTTP Listening Port** in IWSS.
    - **h.** Click **OK** and then **OK** again.
    - **i.** Close Internet Explorer.
5. Login to MSN Messenger.

An error message should appear stating that you were not able to sign into Windows Live Messenger at this time.

6. Disable IntelliTunnel.
   a. Click **HTTP > IntelliTunnel**.
   b. Open the policy.
   c. Unselect **MSN Messenger**.
   d. Click **Save**.
   e. Select the policy and then click **Deploy Policies**.
7. Login to MSN Messenger.

   MSN Messenger should now work.

Note: MSN Messenger uses the proxy configuration in Internet Explorer, so this test should be valid without requiring any modifications to firewalls, network, etc. Other IM applications may not honor the proxy configuration in Internet Explorer and only fall back to port 80 if the standard port is blocked.

About Hot Fixes, Patches, and Service Packs

After an official product release, Trend Micro often develops hot fixes, patches, and service packs to address issues, enhance product performance, or add new features.

The following is a summary of the items Trend Micro may release:

- **Hot fix**: a workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore not released to all customers. Windows hot fixes include a setup program.
- **Security Patch**: a hot fix focusing on security issues that is suitable for deployment to all customers. Windows security patches include a setup program.
- **Patch**: a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Windows patches include a setup program.
- **Service Pack**: a consolidation of hot fixes, patches, and feature enhancements significant enough to be considered a product upgrade. Both Windows and non-Windows service packs include a setup program and setup script.

You can obtain hot fixes from your Technical Account Manager. Check the Trend Micro Knowledge Base to search for released hot fixes:

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

Check the Trend Micro Web site regularly to download patches and service packs:

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

All releases include a readme file with the information you need to install, deploy, and configure your product. Read the readme file carefully before installing the hot fix, patch, or service pack file(s).

Appendix E

Advanced Deployment Functions

Connection Requirements and Properties

Table E-1 below gives the required connections and their properties.

TABLE E-1. Required Connections and Properties

Connecting Component	Traffic: Type and Volume	If the Connection is lost
Clients	Should be measured on the real network	No protection
Database server	**Type:** TDS, a Microsoft proprietary protocol base on TCP. **Volume:** • **Low**—if access logging is disabled • **Medium**—if access logging is enabled	Cached data is used for already started services. Services will not start.
LDAP server (if configured)	**Type:** LDAP **Volume:** Medium	Cached data is used for already started services. Services will not start.
Trend Micro Active Update Server	**Type:** HTTP and HTTPS **Volume:** 10-50 Mb/day	IWSS components cannot be updated in time.

TABLE E-1. Required Connections and Properties (Continued)

Connecting Component	Traffic: Type and Volume	If the Connection is lost
Trend Micro Dynamic Categorization server (if configured)	**Type:** HTTP **Volume:** Depends on the specific access	Requested resources are not categorized properly. URLs prohibited by policy settings can be accessible.
Trend Micro DCS server (if configured)	**Type:** HTTP **Volume:** Depends on the number of infected machines	No cleaning is performed for infected machines.

Throughput and Availability Requirements

The administrator must determine the IWSS availability requirements.

- Is IWSS downtime acceptable?
- If so, what is the proper action (bypass or stop) to enforce when IWSS is down?
- If a failover configuration with multiple IWSS instances is used, do the LDAP server and the database server have the same level of failover?

Hardening Your OS

There are steps you can take before and after your OS installation to harden your OS.

Note: The recommendations in this guide may not fit everyone's needs. Carefully consider your unique environment and situation before implementing these recommendations.

OS Pre-installation Procedures for Hardening

Create your own policy before installing a UNIX or Linux system. The following questions act as a guide to help you create your policy:

- What is the server's primary function?
- Which services and external access ports are required for the majority of uses?
- Who needs access to accounts and to the server?

- What local applications do you need?

Trend Micro recommends that you:

- Start the installation process without a network connection. It is unlikely that your system can be attacked during the installation process if it is not connected to the network.
- Install the latest supported version of your operating system.
- Reconnect only when you are sure that you have taken all the necessary precautions to secure your server.

OS Installation Procedures for Hardening

Most operating system distributions provide the option of a customized installation. However, Trend Micro recommends that you only install the packages that you need and deactivate all the packages that you do not need.

Trend Micro recommends that you partition your hard disk during the installation process. Trend Micro cannot provide partition-sizing requirements because the correct sizing will depend both on your environment and on your plans for the server. Use the following recommendations as a guide:

- Create a dedicated partition for all log files to prevent a Denial of Service (DoS) attack.

Note: By default, IWSS installs the log file into the `/etc/iscan` directory. You need to move the log file location once you have completed the installation.

- If you install a mail host on the server, create a dedicated partition for the mailboxes
- Create a dedicated swap partition that is approximately twice the size of your RAM
- Most UNIX systems have moved to the hierarchical (FHS[2]) filesystem. Check that your partition sizing conforms to this standard.
- The installation process prompts you a password. Take the usual precautions when selecting a password. For example, include digits, meta, and capital characters.
- Create an unprivileged user account to use as your default login.

Post-OS Installation Procedures

Trend Micro recommends that you conduct the following post-installation tasks after completing the installation process:

1. Fortify your system using recommended updates and security patches for all of the installed packages.

   You can download security patches from the following sources:

   - Red Hat™ Linux: http://www.redhat.com/security/
   - SuSE™: http://www.suse.com/us/support/download/updates/index.html

2. Move your system into single-user mode (run level 1 in Linux, run level s in Solaris) when installing patches to minimize the risk of conflicts between running processes and the packages that you are upgrading. Use `init 1` or `s` to change modes.
3. Additionally, you can search at http://www.rpmfind.net for Linux packages. Verify the signature of the files to make sure that the package is original packed by the distributor. Trend Micro recommends that you install SSH for remote administration. Use the following commands to view all installed packages and patches:

   ```
   # rpm -qa
   ```

   For a more detailed description, pipe the result to a more or grep command. For example:

   ```
   # rpm -qa |grep package-name
   ```

4. Remove all unassigned users from `/etc/passwd` (`/etc/shadow`) and from the groups file.

Top Ten UNIX Security Vulnerabilities

Here is a list of the ten top UNIX security vulnerabilities, most of which also apply to Linux:

1. Remote Procedure Calls (RPC)
2. Apache Web Server
3. Secure Shell (SSH)
4. Simple Network Management Protocol (SNMP)
5. File Transfer Protocol (FTP)

6. R-Services -- Trust Relationships
7. Line Printer Daemon (LPD)
8. Sendmail
9. BIND/DNS
10. General UNIX Authentication - Accounts with No Passwords or Weak Passwords[1]

[1] Source: The SANS Institute, December 2002. (www.sans.org)

Protecting a Dedicated Server

Are you protecting an HTTP or FTP Server?

- Used by Internet Service Providers (ISP) or Application Service Providers (ASP) to protect their services
- Network configuration forces clients to contact IWSS instead of the main services by reassigning the DNS-entry to IWSS or using redirection
- No URL filtering or Applet and ActiveX scanning is needed

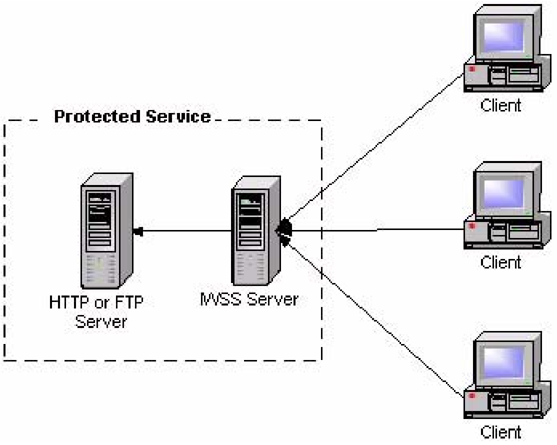


FIGURE F-1 Protecting a Dedicated Server

If you are protecting the HTTP server, install the HTTP scanning service in the HTTP proxy mode and use the reverse proxy configuration.

- Define the following configuration setting in the [http] section of the pni-file
  - `self_proxy=reverse`—specifies operation mode
  - `reverse_server`—specifies the IP address of the protected HTTP server
  - `reverse_server_port`—specifies the TCP port of the protected HTTP server

Note: To simplify the deployment of the reverse-proxy configuration in an HTTP/HTTPS environment, IWSS can listen for the incoming (HTTPS) connection on a port specified by the `[main]/secondaryport` configuration parameter, and forward this traffic without scanning to port 443 of the protected server.

If you are protecting the FTP server, install the FTP scanning service and configure it to use an FTP proxy.

- Define the following configuration setting in the [ftp] section of the pni-file
  - `proxy_mode=dedicated` — specifies operational mode
  - `ftp_server` — specifies the IP address of the protected FTP server
  - `ftp_server_port` — specifies the TCP port of the protected server

Appendix G

Maintenance and Technical Support

This chapter provides information on how to get further assistance with any technical support questions you may have.

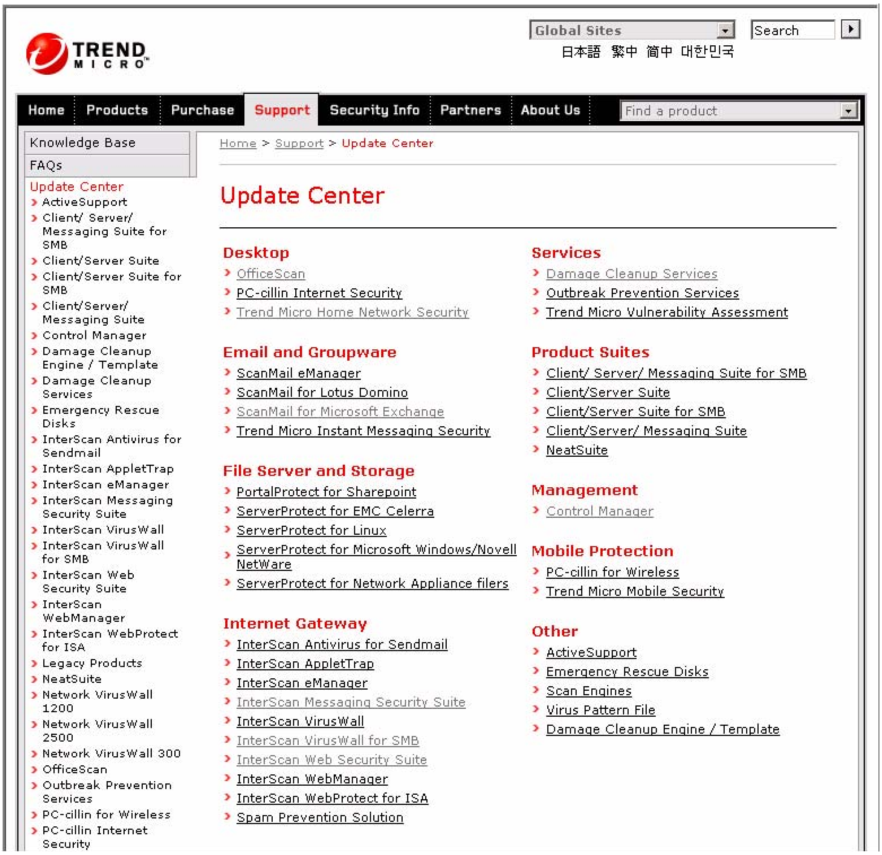
Topics in this chapter include:

Product Maintenance

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

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

The Update Center screen displays. Select your product from the links on this screen:



Update Center

- ActiveSupport
- Client/ Server/ Messaging Suite for SMB
- Client/Server Suite
- Client/Server Suite for SMB
- Client/Server/ Messaging Suite
- Control Manager
- Damage Cleanup Engine / Template
- Damage Cleanup Services
- Emergency Rescue Disks
- InterScan Antivirus for Sendmail
- InterScan AppletTrap
- InterScan eManager
- InterScan Messaging Security Suite
- InterScan VirusWall
- InterScan VirusWall for SMB
- InterScan Web Security Suite
- InterScan WebManager
- InterScan WebProtect for ISA
- Legacy Products
- NeatSuite
- Network VirusWall 1200
- Network VirusWall 2500
- Network VirusWall 300
- OfficeScan
- Outbreak Prevention Services
- PC-cillin for Wireless
- PC-cillin Internet Security

Home > Support > Update Center

Update Center

Desktop

- OfficeScan
- PC-cillin Internet Security
- Trend Micro Home Network Security

Email and Groupware

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

File Server and Storage

- PortalProtect for Sharepoint
- ServerProtect for EMC Celerra
- ServerProtect for Linux
- ServerProtect for Microsoft Windows/Novell NetWare
- ServerProtect for Network Appliance filers

Internet Gateway

- InterScan Antivirus for Sendmail
- InterScan AppletTrap
- InterScan eManager
- InterScan Messaging Security Suite
- InterScan VirusWall
- InterScan VirusWall for SMB
- InterScan Web Security Suite
- InterScan WebManager
- InterScan WebProtect for ISA
- Spam Prevention Solution

Services

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

Product Suites

- Client/ Server/ Messaging Suite for SMB
- Client/Server Suite
- Client/Server Suite for SMB
- Client/Server/ Messaging Suite
- NeatSuite

Management

- Control Manager

Mobile Protection

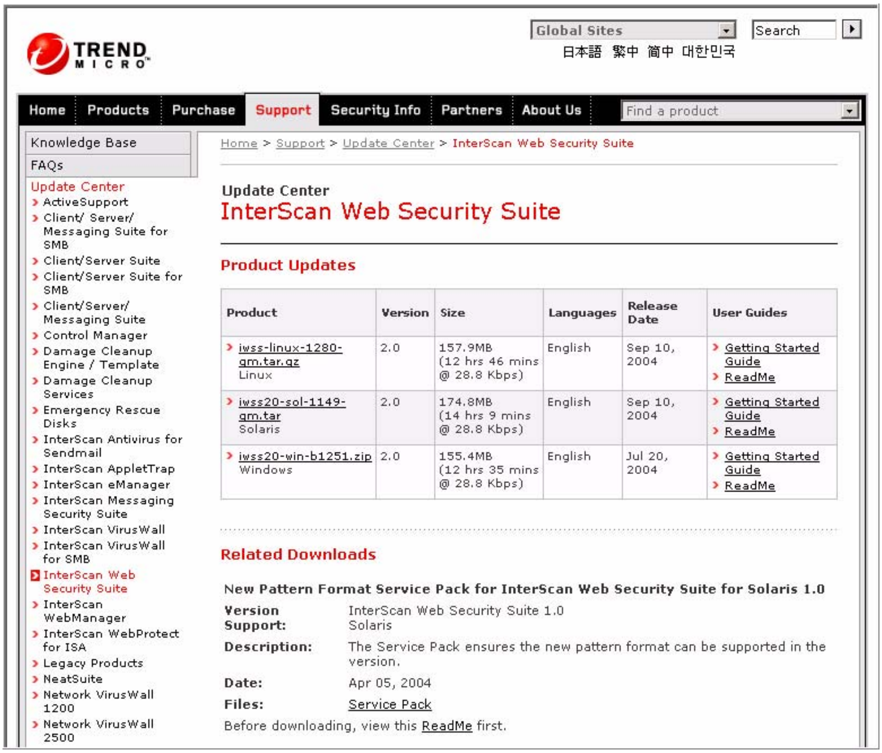
- PC-cillin for Wireless
- Trend Micro Mobile Security

Other

- ActiveSupport
- Emergency Rescue Disks
- Scan Engines
- Virus Pattern File
- Damage Cleanup Engine / Template

FIGURE G-1 Get product and documentation updates from the Update Center

Clicking the link for InterScan Web Security Suite takes you to the Update Center page for IWSS. Scroll down to review the patches that are available.



Update Center

InterScan Web Security Suite

Product Updates

Product	Version	Size	Languages	Release Date	User Guides
iwss-linux-1280-gm.tar.gz Linux	2.0	157.9MB (12 hrs 46 mins @ 28.8 Kbps)	English	Sep 10, 2004	Getting Started Guide ReadMe
iwss20-sol-1149-gm.tar Solaris	2.0	174.8MB (14 hrs 9 mins @ 28.8 Kbps)	English	Sep 10, 2004	Getting Started Guide ReadMe
iwss20-win-b1251.zip Windows	2.0	155.4MB (12 hrs 35 mins @ 28.8 Kbps)	English	Jul 20, 2004	Getting Started Guide ReadMe

Related Downloads

New Pattern Format Service Pack for InterScan Web Security Suite for Solaris 1.0

Version Support: InterScan Web Security Suite 1.0 Solaris

Description: The Service Pack ensures the new pattern format can be supported in the version.

Date: Apr 05, 2004

Files: Service Pack

Before downloading, view this ReadMe first.

FIGURE G-2 IWSS patches available on the Update Center

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

Maintenance Agreement

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support (“Maintenance”) for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro’s then-current Maintenance fees.

Note: If the Maintenance Agreement expires, your License Agreement will not.

If the Maintenance Agreement expires, scanning can still occur, but the product cannot be updated, even manually. Also, you will not be entitled to receive technical support from Trend Micro.

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

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

Renewing Your Maintenance Agreement

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

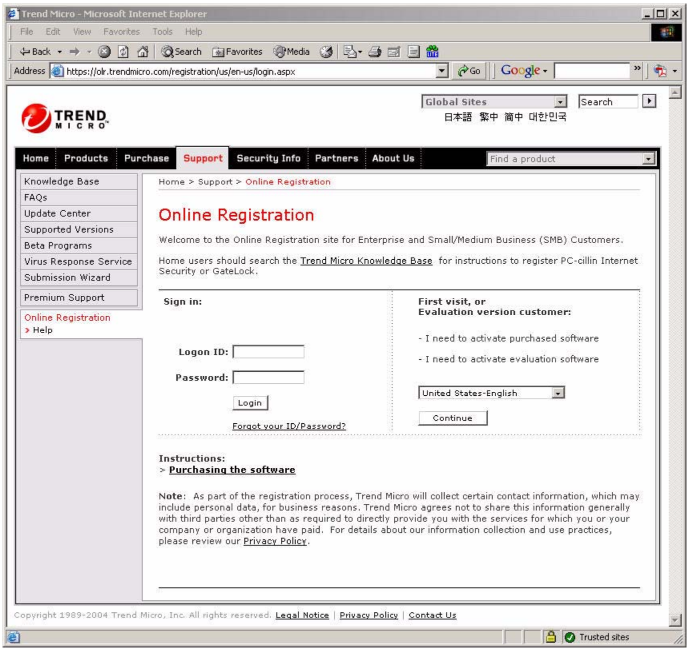
If your Maintenance Agreement expires, scanning will still be possible, but virus pattern and program updates will stop. To prevent this, renew the Maintenance Agreement as soon as possible.

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

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

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

You are prompted to enter a logon ID and password.


Trend Micro - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://olr.trendmicro.com/registration/us/en-us/login.aspx
Go
Google
TREND MICRO
Global Sites
Search
日本語 繁中 簡中 대한민국
Home Products Purchase Support Security Info Partners About Us
Find a product
Knowledge Base
FAQs
Update Center
Supported Versions
Beta Programs
Virus Response Service
Submission Wizard
Premium Support
Online Registration
› Help
Trusted sites

Home > Support > Online Registration

Online Registration

Welcome to the Online Registration site for Enterprise and Small/Medium Business (SMB) Customers.

Home users should search the Trend Micro Knowledge Base for instructions to register PC-cillin Internet Security or GateLock.

Sign in:

Logon ID:

Password:

Login

Forgot your ID/Password?

First visit, or Evaluation version customer:

- I need to activate purchased software

- I need to activate evaluation software

United States-English

Continue

Instructions:
> Purchasing the software

Note: As part of the registration process, Trend Micro will collect certain contact information, which may include personal data, for business reasons. Trend Micro agrees not to share this information generally with third parties other than as required to directly provide you with the services for which you or your company or organization have paid. For details about our information collection and use practices, please review our Privacy Policy.

Copyright 1989-2004 Trend Micro, Inc. All rights reserved. Legal Notice | Privacy Policy | Contact Us

FIGURE 7-3. Trend Micro Online Registration screen.

To view your Registration Profile, type the logon ID and password created when you first registered your product with Trend Micro (as a new customer), and then click **Log on**.

Contacting Technical Support

To contact Trend Micro Technical Support, visit the following URL:

`http://kb.trendmicro.com`

Then, click the link for one of the following regions:

- Asia/Pacific
- Australia and New Zealand
- Europe
- Latin America
- United States and Canada

Follow the instructions for contacting support in your region.

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

`http://www.trendmicro.com`

`support@trendmicro.com`

For regional contact information and the specific technical support numbers for all the regional and worldwide offices, open the IWSS management console and choosing **Support** from the menu in the management console's banner.

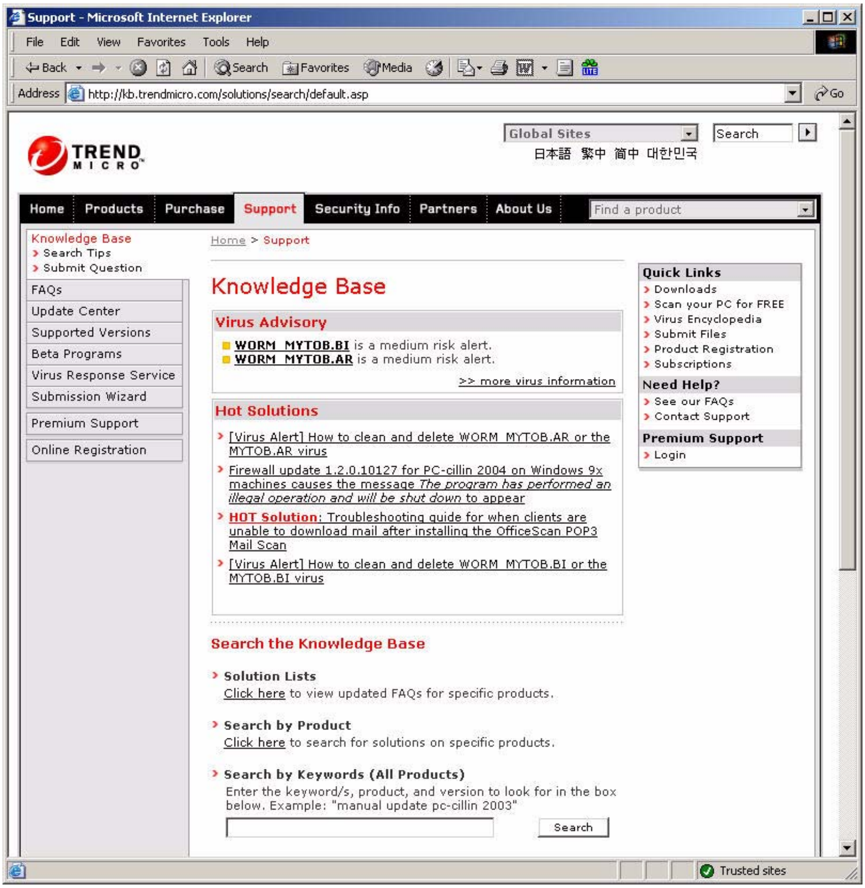
General US phone and fax numbers follow:

`Voice: +1 (408) 257-1500 (main)`

`Fax: +1 (408) 257-2003`

Our US headquarters is located in the heart of Silicon Valley:

```
Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
```



Knowledge Base

Virus Advisory

- **WORM_MYTOB.BI** is a medium risk alert.
- **WORM_MYTOB.AR** is a medium risk alert.

>> more virus information

Hot Solutions

- [Virus Alert] How to clean and delete WORM_MYTOB.AR or the MYTOB.AR virus
- Firewall update 1.2.0.10127 for PC-cillin 2004 on Windows 9x machines causes the message *The program has performed an illegal operation and will be shut down* to appear
- HOT Solution: Troubleshooting guide for when clients are unable to download mail after installing the OfficeScan POP3 Mail Scan
- [Virus Alert] How to clean and delete WORM_MYTOB.BI or the MYTOB.BI virus

Search the Knowledge Base

Solution Lists
Click here to view updated FAQs for specific products.

Search by Product
Click here to search for solutions on specific products.

Search by Keywords (All Products)
Enter the keyword/s, product, and version to look for in the box below. Example: "manual update pc-cillin 2003"

Search

FIGURE G-4 Trend Micro Technical Support site.

TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The “virus doctors” at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging risks. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA, to mitigate virus outbreaks and provide urgent support.

Knowledge Base

The Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do to. New solutions are added daily.

Also available in Knowledge Base are product FAQs, hot tips, preventive antivirus advice, and regional contact information for support and sales.

Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

`http://kb.trendmicro.com`

And, if you can't find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question via an email message. Response time is typically 24 hours or less.

Known Issues

Known issues are features in your IWSS software that may temporarily require a workaround. Known issues are typically documented in section 7 of the Readme document you received with your product. Readme files for Trend Micro products, along with the latest copies of the product manuals, can also be found in the Trend Micro Update Center:

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

Known issues can be found in the technical support Knowledge Base:

`http://kb.trendmicro.com`

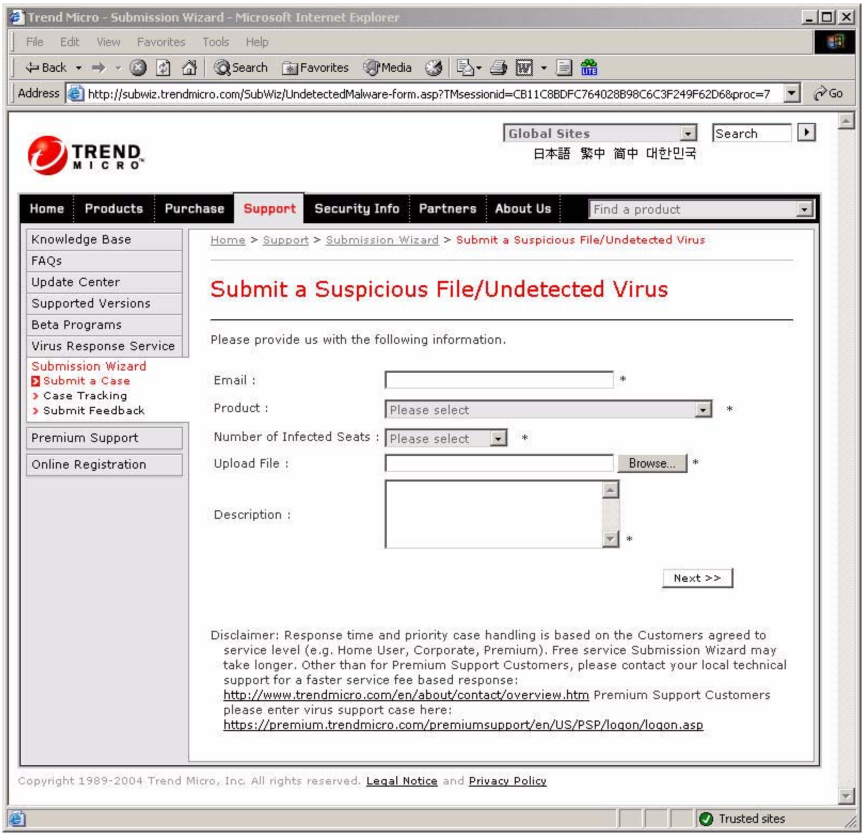
Trend Micro recommends that you always check the Readme file for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

Sending Suspicious Code to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, visit the Trend Micro Submission Wizard URL:

`http://subwiz.trendmicro.com/SubWiz`

Click the “Submit a suspicious file/undetected virus” link. The following screen displays.


Trend Micro - Submission Wizard - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://subwiz.trendmicro.com/SubWiz/UndetectedMalware-form.asp?TMsessionid=CB11C8BDFC764028B98C6C3F249F62D6&proc=7
Go
TREND MICRO
Global Sites
Search
日本語 繁中 简中 대한민국
Home Products Purchase Support Security Info Partners About Us
Find a product
Knowledge Base
FAQs
Update Center
Supported Versions
Beta Programs
Virus Response Service
Submission Wizard
Submit a Case
Case Tracking
Submit Feedback
Premium Support
Online Registration
Trusted sites

Home > Support > Submission Wizard > Submit a Suspicious File/Undetected Virus

Submit a Suspicious File/Undetected Virus

Please provide us with the following information.

Email : *

Product : Please select *

Number of Infected Seats : Please select *

Upload File : Browse... *

Description : *

Next >>

Disclaimer: Response time and priority case handling is based on the Customers agreed to service level (e.g. Home User, Corporate, Premium). Free service Submission Wizard may take longer. Other than for Premium Support Customers, please contact your local technical support for a faster service fee based response: http://www.trendmicro.com/en/about/contact/overview.htm Premium Support Customers please enter virus support case here: https://premium.trendmicro.com/premiumsupport/en/US/PSP/logon/logon.asp

Copyright 1989-2004 Trend Micro, Inc. All rights reserved. Legal Notice and Privacy Policy

FIGURE G-5 Submission Wizard screen

You are prompted to supply the following information:

- **Email**: Your email address where you would like to receive a response from the antivirus team.
- **Product**: The product you are currently using. If you are using multiple Trend Micro products, select the product that has the most effect on the problem submitted, or the product that is most commonly in use.

- **Number of Infected Seats**: The number of users in your organization that are infected.
- **Upload File**: Trend Micro recommends that you create a password-protected zip file of the suspicious file, using the word “virus” as the password—then select the protected zip file in the **Upload File** field.
- **Description**: Please include a brief description of the symptoms you are experiencing. Our team of virus engineers will “dissect” the file to identify and characterize any risks it may contain and return the cleaned file to you, usually within 48 hours.

Note: Submissions made via the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you click **Next**, an acknowledgement screen displays. This screen also displays a case number for the problem you submitted. Make note of the case number for tracking purposes.

If you prefer to communicate by email, send a query to the following address:

`virusresponse@trendmicro.com`

In the United States, you can also call the following toll-free telephone number:

(877) TRENDAV, or 877-873-6328

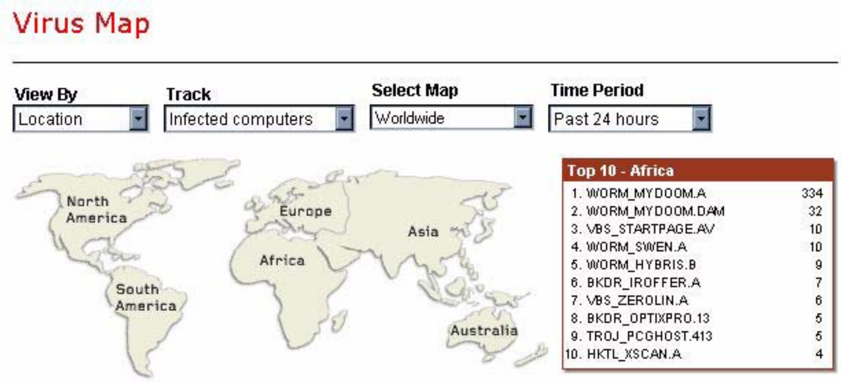
Security Information Center

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

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

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of risks expected to trigger in the current week, and describes the 10 most prevalent risks around the globe for the current week
- View a Virus Map of the top 10 risks around the globe



Virus Map

View By: Location

Track: Infected computers

Select Map: Worldwide

Time Period: Past 24 hours

Top 10 - Africa	
1. WORM_MYDOOM.A	334
2. WORM_MYDOOM.DAM	32
3. VBS_STARTPAGE.AV	10
4. WORM_SWEN.A	10
5. WORM_HYBRIS.B	9
6. BKDR_IROFFER.A	7
7. VBS_ZEROLIN.A	6
8. BKDR_OPTIXPRO.13	5
9. TROJ_PCGHOST.413	5
10. HKTL_XSCAN.A	4

FIGURE G-6 Trend Micro World Virus Tracking Program virus map

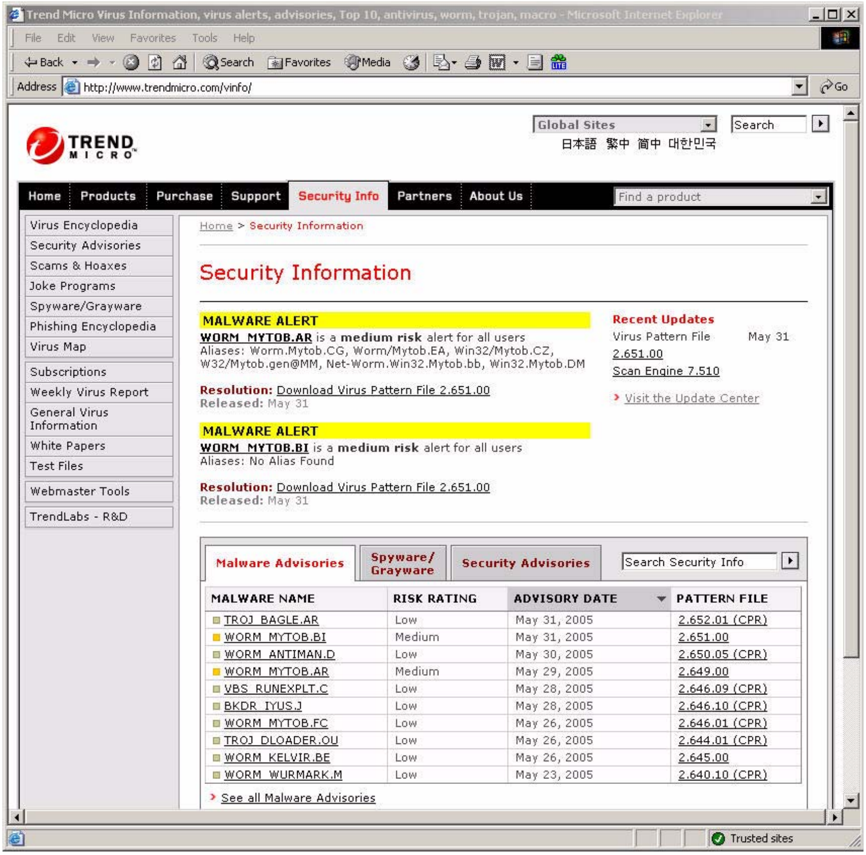
- Consult the Virus Encyclopedia, a compilation of known risks including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the risk, as well as information about computer hoaxes
- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:
    - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other risks
    - The Trend Micro *Safe Computing Guide*

  - A description of risk ratings to help you understand the damage potential for a risk rated Very Low or Low vs. Medium or High risk
  - A glossary of virus and other security risk terminology
- Download comprehensive industry white papers
- Subscribe, free, to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Webmasters
- Read about TrendLabs, Trend Micro's global antivirus research and support center

To open Security Information:

1. Open the IWSS management console.

2. Click **Security Info** from the drop-down menu at the top-right panel of the screen. The **Security Information** screen displays.


Trend Micro Virus Information, virus alerts, advisories, Top 10, antivirus, worm, trojan, macro - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.trendmicro.com/vinfo/
Go
TREND MICRO
Global Sites
Search
日本語 繁中 简中 대한민국
Home Products Purchase Support Security Info Partners About Us
Find a product
Virus Encyclopedia
Security Advisories
Scams & Hoaxes
Joke Programs
Spyware/Grayware
Phishing Encyclopedia
Virus Map
Subscriptions
Weekly Virus Report
General Virus Information
White Papers
Test Files
Webmaster Tools
TrendLabs - R&D
Trusted sites

Home > Security Information

Security Information

MALWARE ALERT

WORM_MYTOB.AR is a **medium risk** alert for all users
Aliases: Worm.Mytob.CG, Worm/Mytob.EA, Win32/Mytob.CZ, W32/Mytob.gen@MM, Net-Worm.Win32.Mytob.bb, Win32.Mytob.DM

Resolution: Download Virus Pattern File 2.651.00
Released: May 31

MALWARE ALERT

WORM_MYTOB.BI is a **medium risk** alert for all users
Aliases: No Alias Found

Resolution: Download Virus Pattern File 2.651.00
Released: May 31

Recent Updates
Virus Pattern File 2.651.00 May 31
Scan Engine 7.510

› Visit the Update Center

Malware Advisories | Spyware/Grayware | Security Advisories | Search Security Info

MALWARE NAME	RISK RATING	ADVISORY DATE	PATTERN FILE
TROJ_BAGLE.AR	Low	May 31, 2005	2.652.01 (CPR)
WORM_MYTOB.BI	Medium	May 31, 2005	2.651.00
WORM_ANTIMAN.D	Low	May 30, 2005	2.650.05 (CPR)
WORM_MYTOB.AR	Medium	May 29, 2005	2.649.00
VBS_RUNEXPLT.C	Low	May 28, 2005	2.646.09 (CPR)
BKDR_IYUS.J	Low	May 28, 2005	2.646.10 (CPR)
WORM_MYTOB.FC	Low	May 26, 2005	2.646.01 (CPR)
TROJ_DLOADER.OU	Low	May 26, 2005	2.644.01 (CPR)
WORM_KELVIR.BE	Low	May 26, 2005	2.645.00
WORM_WURMARK.M	Low	May 23, 2005	2.640.10 (CPR)

› See all Malware Advisories

FIGURE G-7 Trend Micro Security Information screen.

About Trend Micro

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

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

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

`http://www.trendmicro.com`

Index