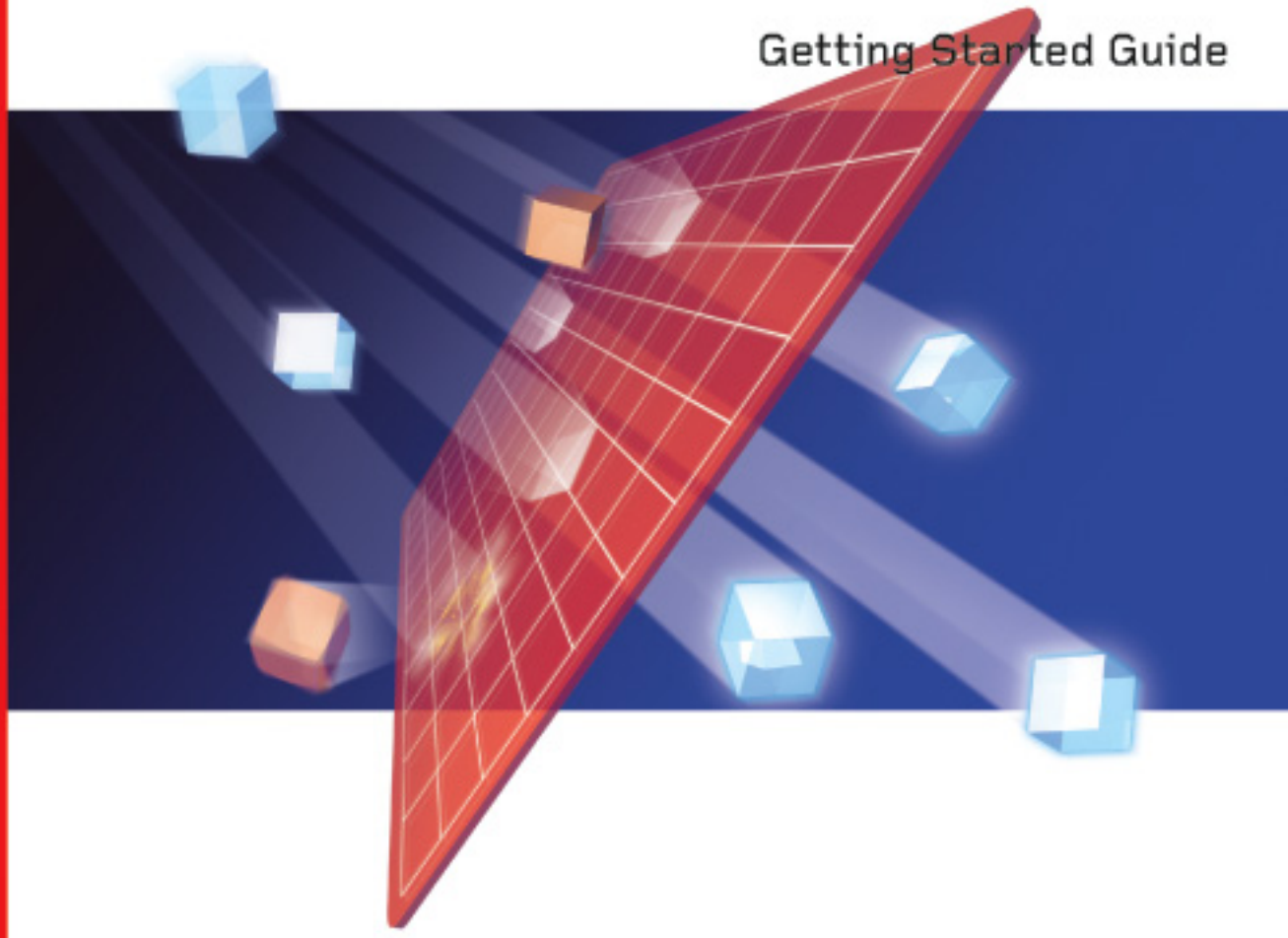
TREND MICRO™
InterScan™2 Web Security Suite

High performing, scalable gateway Web security for the enterprise

for Linux™ and Solaris™

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

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

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.

RSA Data Security, Inc. MD5 Message-Digest Algorithm
Copyright (C) 1991-1992, RSA Data Security, Inc. Created 1991. All rights reserved. License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

Cryptographic software written by Eric Young and Tim Hudson
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

OpenSSL License Agreement
Copyright (c) 1998-2001 The OpenSSL Project. All rights reserved. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

STLport software.
Copyright 1999-2000 Boris Fomitchev. This material is provided as is, with no warranty expressed or implied. Any use is at your own risk. Permission to use or copy this software for any purpose is hereby granted without fee provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.
Copyright 1994 Hewlett-Packard Company. Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.
Copyright 1996-1997 Silicon Graphics Computer Systems, Inc. Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.

ICU License - ICU 1.8.1 and later

JFreeChart

PostgreSQL

Document Part No. IHEM22346/50718

Release Date: September 2005

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

The Getting Started 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 must read through it prior to installing or using the software.

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

Chapter 3: Installation and Setup

Chapter 1

Introducing InterScan™ Web Security Suite

Web traffic exposes corporate networks to many potential security threats. While a majority of computer viruses enter organizations through messaging gateways, Web traffic is an increasing method of travel for new threats. For example, mixed threats, which take advantage of multiple entry points and vulnerabilities, can use HTTP to spread.

Significant assessment, restoration, and lost productivity costs associated with outbreaks can be prevented. InterScan Web Security Suite (IWSS) is a comprehensive security product that protects HTTP and FTP traffic in enterprise networks from viruses and other threats.

In addition to antivirus protection, IWSS also helps you with other network management problems. For example, the URL filtering feature enables you to block URLs that may expose your organization to liability. The PhishTrap service protects against phishing, which is a fraudulent collection of confidential information.

Trend Micro™ InterScan™ Web Security Suite (IWSS) is a highly scalable and reliable Web security solution. IWSS is designed to deliver best in class URL filtering and HTTP and FTP virus scanning. IWSS leverages the administration, policy, and centralized management of the Trend Micro Enterprise Protection Strategy (see *About EPS* starting on page 1-19 for more information). This chapter provides an overview of IWSS features and benefits.

Topics included in this chapter are:

- Why URL Filtering?
- How InterScan Web Security Suite Scans Files
- InterScan Web Security Suite Illustration
- How InterScan Web Security Suite Detects Viruses
- Benefits of InterScan Web Security Suite
- Main Features
- About Viruses
- About EPS
- Using the Product Documentation

In addition to this Getting Started Guide, see the context-sensitive online help for more information. Online help is available when you click the help icon () from most screens in the IWSS console.

Overview

IWSS can provide a high degree of user configurability. For example, you can schedule routine tasks such as virus alert notifications and virus, spyware, and PhishTrap pattern updates to occur automatically—just "set and forget." You can also determine which file types are scanned for viruses, the action that IWSS takes when a virus or other security risk is detected (clean, delete, quarantine, or pass), and other program details.

As an added security check, and to leverage the routing of all Web traffic through IWSS for virus scanning, URL filtering is available with IWSS. IWSS provides URL access control management based on content category. You can also integrate IWSS with existing user and group information to provide user-based policy management. IWSS provides security for executable code that is accessed via HTTP and prevents outbound access via HTTP to sites identified as malicious by TrendLabs. IWSS provides reporting and auditing capabilities and supports multiple server configurations.

Why URL Filtering?

When the Internet became widely available in the workplace, pornographic Web sites were so frequently visited as to create a significant legal liability. A hostile work environment could easily be created, with sexual harassment lawsuits following. Although pornographic sites are still commonly visited from the workplace, a myriad of new Internet-based distractions now compete for employee time. Internet shopping, online stock trading, auction bidding and selling, searching for outside employment opportunities and the resource-intensive downloading of MP3 music files and streaming audio and video all tempt employees. This reduces employees' productivity and available bandwidth.

IWSS URL filtering allows the Internet to be made available to corporate users according to user and workgroup-specific needs. You can manage an employee's Internet access by specifying URL filtering policies for all users (or a specific user), all groups (or a specific group), an IP address (or range of IP addresses) and hostname, thus, optimizing individual employees' use of the Internet. IWSS classifies the content of Web pages into over fifty categories. Web sites are grouped and classified into the following URL categories:

- Company Prohibited Sites

- Not Work Related
- Possible Research Topics
- Business Function Related
- Customer Defined
- Others

A default policy prevents access to a configurable set of category groups. You can create additional policies to allow access to restricted category groups (that is, for users with job functions that require broader access). For example, members of the Human Resources department may need unrestricted Internet access to conduct investigations into violations of their company's acceptable use policies.

How InterScan Web Security Suite Scans Files

IWSS is designed to scan HTTP and FTP traffic for viruses at the Internet gateway. IWSS scans files smaller than the set in-memory scan size (64KB by default). However, for files larger than the set in-memory scan size, IWSS copies the file to a temporary location and scans it. If the file is clean, IWSS deletes the copy and forwards the original to its destination. If a virus is detected, a warning message appears, a notification is sent, and IWSS takes one of the following configurable actions:

- **Quarantine** the infected file (without cleaning); the requesting client will not receive the file
- **Delete** the infected file; the requesting client will not receive the file
- **Clean** the infected file; the requesting client will receive the cleaned file if it is cleanable

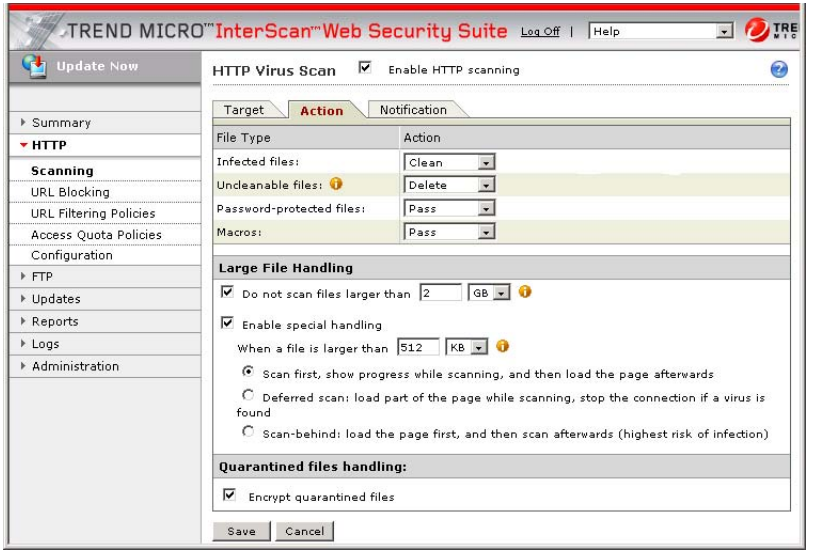


FIGURE 1-1. You can configure the scan action settings for both HTTP and FTP traffic—HTTP is shown in the above example.

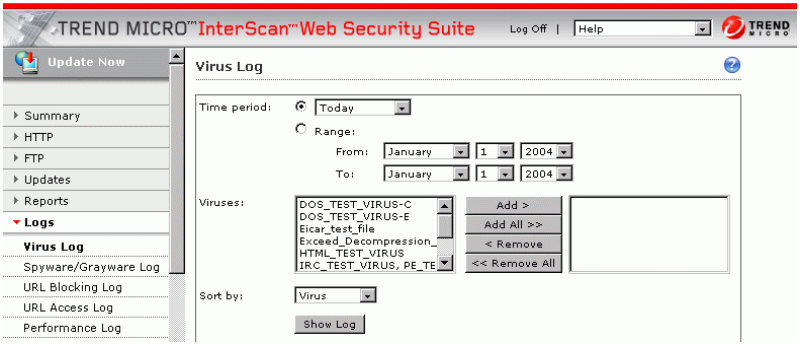
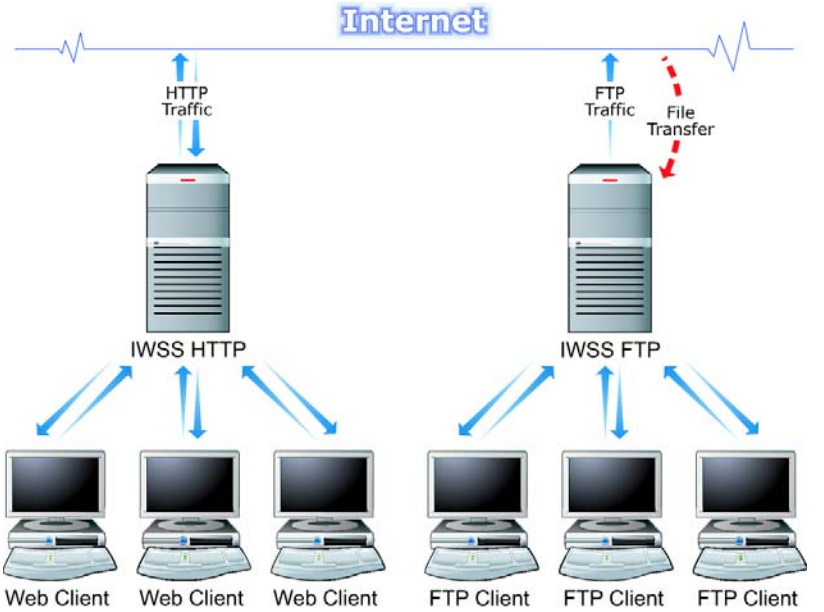


FIGURE 1-2. IWSS is also designed to record virus events and associated actions in the log.

InterScan Web Security Suite Illustration

The following is a conceptual model of how traffic moves between the Internet and Web or FTP clients protected by IWSS.



How InterScan Web Security Suite Detects Viruses

Using a process called “pattern matching,” IWSS draws on an extensive database of virus patterns to identify known viruses. IWSS examines key areas of files for characteristic strings of virus code and compares them against the tens of thousands of virus signatures that are contained in a pattern file.

After the binary patterns in the file are compared against the virus pattern file and the scan engine found that the file is infected, IWSS takes the action you specify: clean, delete, or quarantine. Some malicious code cannot be cleaned, and the actions for this type of incident are delete, quarantine, or pass (deliver anyway; this action is not recommended).

It is important to keep the virus, PhishTrap, and spyware pattern files up-to-date. Trend Micro makes it easy to update these components by supporting automatic updates. See *Updating the Virus Pattern File* starting on page 3-32 for more information.

Compressed Files

IWSS opens and examines the contents of compressed files based on the criteria specified in the **HTTP Virus Scan** and **FTP Virus Scan** screens. IWSS performs decompression according to the configurable limits (number of files, decompression percent, decompressed file size, and decompression layers). See *Configuring Compressed File Scanning Limits* starting on page 4-17 and 6-5 for more information.

Benefits of InterScan Web Security Suite

Trend Micro InterScan Web Security Suite offers powerful protection for your organization's HTTP and FTP gateway traffic. The major benefits available with this product include:

Integration with ICAP 1.0-compliant Caching Devices

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

Centralized Management via Trend Micro Control Manager™

InterScan Web Security Suite works with the Trend Micro Control Manager (see *Trend Micro Control Manager* starting on page 9-1) administration console to provide centralized management and enterprise-wide coordination for Trend Micro products and services. Trend Micro Control Manager acts as a command center for deployment of industry-unique services that deliver TrendLabs^{SM} expertise to critical points across the network (see *TrendLabs* starting on page 10-9 for more information).

Supports Outbreak Prevention Services

InterScan Web Security Suite also supports Trend Micro Outbreak Prevention Services, subscription-based services that deliver outbreak prevention policies and attack-specific information to critical network access points, before the release of a pattern file. With Outbreak Prevention Services, outbreak prevention policies can be centrally deployed to automatically block, isolate, and contain an outbreak. By accelerating response time to new viruses and other security risks, enterprises can contain outbreaks faster, minimize system damage, and prevent downtime.

Efficient URL Filtering and Reporting Function

IWSS URL filtering reduces legal liability. It also increases employees' productivity and available bandwidth. It allows the Internet to be optimally managed for corporate users according to user and workgroup-specific needs. You can manage employee Internet access by specifying the URL filtering policies for all users (or a specific user), all groups (or specific groups), IP address (or range of IP addresses) and hostname. Also, IWSS offers configurable, real time and scheduled reports for viewing activity within the entire environment, a group of users, or a specific user's activity.

Comprehensive Virus Protection

InterScan Web Security Suite:

- Protects against mixed-threat attacks such as Nimda and its variants, which take advantage of multiple entry points and vulnerabilities in enterprise networks
- Provides numerous virus scanning and security options, including scanning and automatic cleaning (when possible) of HTTP and FTP virus-infected file transfers
- Uses both rule-based and pattern recognition technologies to detect known and unknown viruses
- Includes MacroTrap™ and ScripTrap™ heuristic scanning feature to detect and remove known and unknown macro and script viruses

Main Features

InterScan Web Security Suite helps you manage your HTTP and FTP traffic in the following ways:

URL Filtering

Enables enterprises to reduce corporate liability and bandwidth costs while maintaining solid security policy practice.

Active Directory Integration

Helps leverage the enterprise's current network management infrastructure by reducing the amount of overhead associated with deploying new security solutions.

Policy Management Structure

Provides easy-to-use policy management tools for applying new applications to users and groups within the enterprise.

Enhanced Reporting

Offers configurable, real time and scheduled reports for viewing activity within the entire environment, for a group of users, or for a specific user's activity.

PhishTrap

Protects the enterprise and its employees from becoming victims of spoofs and scams by preventing access to known phishing URLs.

Spyware

Leverages new scan engine functions and the new spyware pattern file to detect spyware programs at the gateway, before they are passed to the end user.

New, Streamlined User Interface

Offers an easier way to navigate configuration settings, reducing the amount of time needed to set up or refine policies.

Large File Handling

Offers options for handling large files to avoid browser time-outs or the appearance of a hung connection. Once it encounters a large file, IWSS can handle it in one of the following ways: (1) deliver the data from the file to the user and scan later (scan-behind), (2) generate a progress page to prevent the browser from having a timeout issue, or (3) load part of the page while scanning, and then stop the connection whenever a virus is found (deferred scan).

MIME Encoding

Bypasses certain MIME content-types (see *Understanding Scan Configuration Options* starting on page 4-2 for information on the benefit of bypassing certain MIME content-types). However, this is not a practice that Trend Micro recommends when you enable the large file special handling option, because it is possible to imitate a MIME content-type. However, if you are unable or choose not to enable large file handling, IWSS must act upon the entire file. Some file types, such as RealAudio or other streaming content, begin playing as soon as the first part of the file reaches the client machine and will not work properly with the resulting delay. You can have IWSS omit these file types from scanning by adding the appropriate MIME content-types to the list of MIME content-types to skip.

Macro Scan

Helps prevent virus outbreaks by giving you the option to quarantine all attachments containing macros, regardless of whether they have viruses, or to remove the macro and deliver the attachment as usual.

During the early stage of a new macro virus outbreak, there may be times when you want to stop all macro-containing documents from entering your network. Macro scan can stop all attachments with macros from entering the LAN and crossing the Internet gateway, until a new pattern file becomes available.

File Types to Block

Blocks the transfer of types of files that you do not want your users to retrieve, such as Java applets, executable files, Microsoft Office documents, compressed files, audio/video files, graphics, and so on. The message that the user sees when IWSS blocks a file is configurable. In addition, a notification email message can be sent when IWSS blocks a file. IWSS does not block files retrieved through peer-to-peer file sharing programs because these services use their own protocols and do not use HTTP. However, IWSS can screen the Web sites associated with these services.

File Types to Scan

Scans all file types, scans file types with specified extension, or scans files using IntelliScan™, which checks the true file-type of a file regardless of its extension to determine whether to block or scan it. True file-type identification offers more comprehensive file type protection if you are using IntelliScan or the scan all file types option (see *True File Type* starting on page 4-16 for more information).

Web Site and URL Strings Blocking

Blocks Web sites and URL strings in both ICAP and HTTP proxy mode (see *Protocol Handlers* starting on page C-2). You can explicitly specify the Web sites and URL strings to block (or to exempt from blocking). Using this feature, you can block a given site, yet still allow accessing some of its sub-sites.

Scanning of HTTP Post Content

Scans HTTP POST content (for example, Web mail attachments). This feature works in both ICAP and HTTP proxy mode (see *Protocol Handlers* starting on page C-2). IWSS provides scanning of HTTP requests as well as responses to limit the spread of viruses and to identify local machines that attempt to pass an infected file over HTTP. The most common type of HTTP request that can contain malicious content is the POST request with a multipart/form-data content-type; for content-types other than a multipart/form-data, IWSS scans the posted content as a single document. IWSS scans each section of a multipart POST, and then replies to the client with a 403 response if any section contains infected or uncleanable data. IWSS logs the event and the origin of the infected request as well. If you set the scan action option to **Clean** and you encounter a cleanable file, IWSS cleans that section before being passed to the remote host. IWSS also scans content passed via HTTP PUT or

FTP-over-HTTP PUT. Request scanning does not support special handling of large files (that is, scan-behind, deferred scan, or progress page).

Preview Scanning

Offers a reliable way to skip files that do not need scanning. For MIME content-types that are not excluded on the configuration screen, IWSS inspects the first 4KB of a file to determine if its content is a safe type. If the scan engine indicates that the file is not of a type that can harbor viruses, the data is passed on to the client without further inspection. In general, the performance benefit from skipping safe files more than offsets any additional processing cost.

FTP Scanning

Supports FTP scanning to prevent viruses from entering the network through FTP file transfers. You can either use FTP scanning to protect a local FTP site or for screening files that users access via IWSS acting as their FTP proxy. See *FTP Installation Topology* starting on page 2-13 for more information.

Comprehensive Log Files

IWSS provides two types of logs; Reporting Logs and System Logs. There are multiple types of each: HTTP scan, FTP scan, Mail delivery service, Administration, and Update logs are examples of system logs; and Virus, Spyware/Grayware, URL Blocking, Performance, and URL Access logs are examples of reporting logs. System logs contain unstructured messages due to errors or state changes in the software, and are only visible by viewing the log file— they cannot be seen from the Web console. Reporting logs provide program event information, and can be viewed in the IWSS console.

Tracing Security Events Back to Affected Systems

Warns of the presence of an infected file on a client system. This can happen either when an infected file is posted to the Web or when a large file is scanned after IWSS has delivered it to the client, and the scan discovers an infected file. When IWSS detects a virus on a client system, you must identify the system and perform a cleanup. IWSS uses three methods to identify the infected system: host name (modified HTTP headers), user/group name, or IP address.

FIGURE 1-3. IWSS can identify users via IP address, host name (modified HTTP headers), or user/group name via proxy authentication.

What's New in IWSS 2.2

This version of Trend Micro InterScan Web Security Suite (IWSS) provides the following new features:

- A new tab on the **Summary** screen now allows you to view frequency of spyware and grayware detections today, in the past week, and in the past month.
- A new tab on the **Summary** screen now allows you to view a bar chart called the Threat Report, which displays frequency of detections by threat type—spyware/grayware, virus, Trojan, worm, macro, phish, unsigned ActiveX, and URL filter violations.
- Real-time and scheduled reports have been enhanced to include information about:
  - Spyware/grayware cleanup by category
  - Top spyware/grayware detections

  - Most infected users
- A new log (the Spyware/Grayware Log) is available in this release. You can select spyware or grayware by name and show a report of detections during a specified period with this new log.
- The required number of semaphore undo structures (SEMMNU) for process mode installs running on Solaris has increased.

About Viruses

A computer virus is a program that replicates. To do so, the virus needs to attach itself to other program files (for example, .exe, .com, .dll) and execute whenever the host program executes.

Beyond simple replication, a virus almost always seeks to fulfill another purpose: to cause damage. Called the damage routine, or payload, the destructive portion of a virus can range from overwriting the partition table on the main system disk to scrambling the numbers in your corporate spreadsheets to just taunting you with sounds, pictures, or effects.

It's worth bearing in mind, however, that even without a "damage routine," left unabated, viruses continue to propagate—consuming system memory, disk space, slowing network traffic, and generally degrading performance. Virus code can be the source of mysterious system problems that take weeks to understand.

Some viruses, in conjunction with "logic bombs," do not make their presence known for months. Instead of causing damage right away, these viruses do nothing but replicate—until the preordained trigger day or event when they unleash their damage routines across the network.

Whether it was written to be harmful or just annoying, a virus on your system can lead to instability and should not be allowed to remain.

Virus Writers

In the traditional scenario, a highly-technical individual, working alone, would write a virus program and then introduce it onto a computer, network server, or the Internet. Why? Ego, revenge, sabotage, and basic disgruntlement have all been cited as motivations for virus writers.

Now, however, it takes no special skill to create a macro virus, a mass mailer, or other virus with highly disruptive potential. In fact, “virus kits” proliferate on the Internet and are available at no cost to anyone who wants to try disrupting the Internet or corporate communications.

About Virus Scanning

At the root of antivirus programs such as IWSS are both a scan engine and a comprehensive database of virus “signatures,” commonly called the virus pattern file. Together, these two components do the work of identifying and then cleaning infected files.

At its most basic, a gateway antivirus application monitors HTTP and FTP traffic between the LAN and the Internet. Whenever it detects a file type that it has been configured to scan (for example, .zip, .exe, .doc, and so on), the application copies the file to a temporary location and opens the copy for virus checking.

If the file is clean, the application deletes the copy and releases the original for delivery to the FTP or HTTP server, which delivers the file as usual. If a virus is detected, the application takes whatever action it has been configured to take: *clean*, *delete*, *quarantine*, or *pass* (deliver anyway - this choice is not recommended). *Deleted* and *quarantined* files are not delivered to the requesting client. Files set to be *cleaned* are opened, the virus code removed, and the file is then reassembled.

Not all viruses, or malware, can be cleaned. For example, some viruses corrupt the host file, making it unusable. Trojans, worms, and mass mailers do not “infect” a host file and therefore cannot be cleaned. Whatever the action, all detections are written to the virus log; the administrator and/or designated others can also receive an automatic notification of the incident.

About ActiveUpdate

ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, anti-spam rules, and program files via the Internet.

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

Updated components are also available on the Trend Micro Total Solution CD, which is issued quarterly to customers on Premium Support.

Updating with Trend Micro Control Manager

Trend Micro Control Manager continuously polls the ActiveUpdate server on a regularly scheduled basis. When an update is available, Control Manager downloads the updated component to the Control Manager server.

The update is then deployed to the managed products according to your Control Manager configuration, which could include:

- Manually deploy on-demand
- Automatically deploy immediately after the download
- Deploy according to a deployment plan, for example, certain servers are prioritized for an update

Updating without Trend Micro Control Manager

If you are not using Control Manager for centralized administration of your Trend Micro products, IWSS can be configured to poll the ActiveUpdate server directly. Updated components are deployed into IWSS on a schedule you define.

Note: New threats appear every day. Trend Micro recommends at least daily updates.

Incremental Updates of the Virus Pattern File

ActiveUpdate supports incremental updates of the virus pattern file. Rather than download the entire 5-6MB pattern file each time, ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file. For networks running hundreds of individual desktop products, incremental updates can save considerable bandwidth.

About Heuristic Virus Protection

The Trend Micro scan engine uses two methods for detecting viruses, worms, Trojans, and other Internet security threats: pattern matching and heuristic scanning.

1. **Pattern matching**—as the engine checks each file, it compares the binary file data to a list of known virus "signatures" or strings of code. Pattern matching is thorough and efficient, but is limited to detecting only known viruses
2. **Heuristic scanning**—as the engine checks each file (or email message), it runs through a series of "questions" to analyze whether the file possesses the characteristics of a threat. Because heuristic scanning is an evaluative method rather than comparative, it excels in detecting undiscovered viruses and threats, including polymorphic viruses—those that change "signatures" with each new infection.

   Trend Micro heuristic scanning includes the following specialized technologies:

   - **ScriptTrap**—Detects script-based viruses including JavaScript, Visual Basic (VB) Script, HTML, and Active Server Pages (ASP) Scripts
   - **Vice Engine**—Detects new and unique Denial of Service (DoS) threats
   - **MacroTrap**—Detects unknown macro viruses—including those embedded in the following types of files: Microsoft Word, Excel, PowerPoint, Access, Visio, and Microsoft Project
   - **Softmice**—Detects complex polymorphic viruses using a 32-bit emulator to fool the virus into revealing itself in a safe and contained environment
   - **BootTrap**—Detects both boot sector and partition table viruses

About the Trend Micro Scan Engine

At the heart of all Trend Micro products lies a proprietary scan engine. Originally developed in response to the very first computer viruses the world had seen, the scan engine today is exceptionally sophisticated and capable of detecting Internet worms, mass-mailers, Trojan horse threats, phish sites, spyware, and network exploits, as well as viruses. The scan engine detects threats known to be:

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

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

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

In addition, the scan engine is able to decrypt all major encryption formats (including MIME and BinHex). It also recognizes more than 30 compression formats, including Zip, Arj, and Cab. Most Trend Micro products also allow the product administrator to determine how many layers of compression to scan (up to a maximum of 20), for compressed files contained within a compressed file (see *Platforms, Compression, and Encoding* starting on page D-1 for more details).

It is important that the scan engine remain current with breaking threats. Trend Micro ensures this in two ways:

1. Frequent updates to the scan engine's data-file, called the virus pattern file, which can be downloaded and read by the engine without the need for any changes to the engine code itself
2. Occasional technological upgrades in the engine software, typically prompted by a paradigm-shift in the nature of virus threats, for example the recent rise in mixed-threats such as SQL Slammer and the so-called network viruses

In both cases, updates can be scheduled from the antivirus product to occur automatically, or they can be manually handled by the administrator in charge of security.

The Trend Micro scan engine is certified annually by international computer security organizations, including ICSA.

About EPS

Trend Micro Enterprise Protection Strategy, or EPS, protects against virus outbreaks and mixed-threat Internet attacks, such as mass-mailing worms, Trojans, Denial of Service (DoS) attacks, and unique network exploits such as the Slammer worm. The Enterprise Protection Strategy is delivered in three phases; Outbreak Prevention, Virus Response, and Assessment & Restoration:

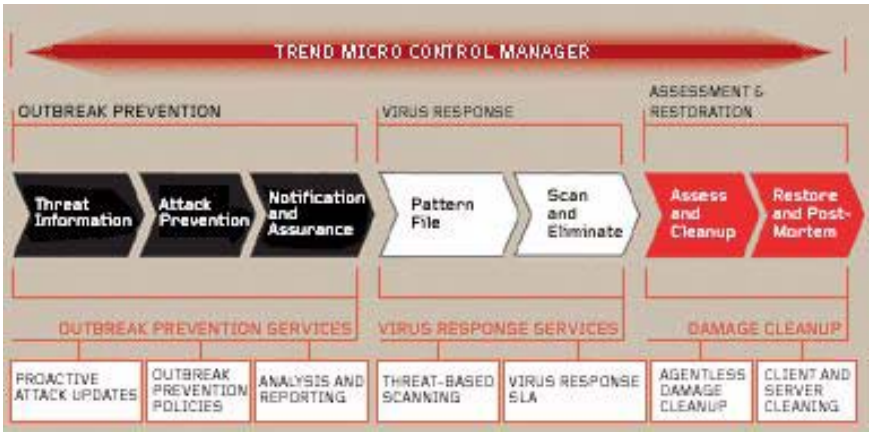


FIGURE 1-4. Enterprise Protection Strategy.

- **Outbreak Prevention**—By closely monitoring Internet security events, TrendLabs (Trend Micro's global research arm), can:
  - Alert administrators
  - Immediately begin deploying a preventive solution called Outbreak Prevention Services (OPS)
- **Virus Response**—Solutions are deployed:

  - From Trend Micro to Control Manager, Trend Micro's central management console
  - From Control Manager to subscribed antivirus products installed on the gateway, mail servers, network servers, and desktops
- **Assessment and Restoration**—Damage assessment and cleanup (if needed) takes place, to:
  - Identify and remove dangerous viruses, worms, and Trojan remnants that can re-attack your network
  - Help rid your system of hidden guest accounts, registry entries, or memory-resident payloads
  - Highlight areas where your networks are most vulnerable

Example Scenario

Assume that:

1. The first signs of a unique new mixed-threat exploit begin appearing at dawn in the Netherlands.
2. TrendLabs immediately starts analyzing the threat to break down its behavior and characteristics. They find that the threat is a mass-mailer worm that drops a Trojan, which hijacks a port in the network. It then begins using the port to contact a given IP address.
3. Within two hours, TrendLabs has released a multi-tiered solution:
   - Blocking the email message containing the worm
   - Scanning the network for the Trojan, and
   - Closing the vulnerable port
4. The solution is certified and released to subscribers.
5. For any network that may already be exposed, a clean-up routine is launched.

If attacks are caught in the OPS phase, EPS subscribers are often able to avoid damage, downtime, and cleanup efforts.

Using the Product Documentation

The documentation set for this product includes the following:

- Getting Started Guide—This Guide helps you get “up and running” by introducing IWSS, assisting with installation planning, implementation, and configuration, and describing the main product functions. It also includes instructions on testing your installation using a harmless test virus. The latest version of the Guide is available in electronic form at:

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

- Online help—The purpose of online help is to provide “how-tos” for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online help is accessible from the IWSS user interface.
- 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.
- Knowledge Base— The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, open:

  `http://kb.trendmicro.com`

Chapter 2

Installation Planning

This chapter presents an installation planning summary and different topologies for each IWSS protocol handler.

Topics included in this chapter are:

- Installation Planning Summary
- Recommended System Requirements
- HTTP Proxy Topology
  - Deploying HTTP in a Multiple Server Configuration
  - IWSS HTTP Stand-alone Installation Topology with Multiple Servers
  - IWSS ICAP Installation Topology with Multiple Servers
- FTP Installation Topology
  - Stand-alone Mode
  - Local FTP server
  - Upstream FTP Proxy
- Report and Database Setup
- User Identification Process
- Notes on User/Group Name via Proxy Authorization

Installation Planning Summary

IWSS 2.0 supports upgrading from IWSS 1.0 and is capable of importing the exceptions list from InterScan WebManager. After installing IWSS, install the Control Manager agent if you are using Control Manager (see *Control Manager Overview* starting on page 9-2 for more information).

Note: Trend Micro recommends that IWSS be installed on a dedicated server.

Select the components that you want to install:

- InterScan Web Security Suite HTTP
- InterScan Web Security Suite FTP
- InterScan Web Security Suite URL Filter

URL filtering requires a separate Activation Code to be functional. You also need to decide on the type of database to use and whether you run the database on the IWSS system or in a central location:

- PostgreSQL 7.4.1, which is installed with IWSS or
- Oracle 8i/9i

Also, you need to define your user identification mechanism (see *User Identification Process* starting on page 2-18 for more details):

- Identify by the IP address
- Host name (modified HTTP headers)
- User/group name via proxy authorization (use LDAP for account information)

For InterScan Web Security Suite HTTP Scanning

Choose the type of IWSS HTTP handler you will use (for information on how to identify the type of IWSS HTTP handler, see *Protocol Handlers* starting on page C-2):

- ICAP
- Proxy Scan

Note: Choose ICAP if there is already a content-cache server on your network.

Under Proxy Scan, you can configure HTTP Proxy as either **Stand-alone mode** (if you are not using an upstream proxy) or **Dependent mode** (if you are using an upstream proxy) in the configuration screen (**HTTP > Configuration > Proxy Scan**) of the IWSS console. See *HTTP Proxy Topology* starting on page 2-7 for more information. For **Dependent mode**, specify the proxy name and port number. **Dependent mode** requires the use of additional hardware (proxy server); however, it supplements the existing HTTP proxy for other features such as caching, logging, filtering, and network configuration.

For InterScan Web Security Suite FTP Scanning

You can set up the IWSS FTP service to run in one of the three settings available:

- Stand-alone
- Local FTP server
- Upstream FTP proxy

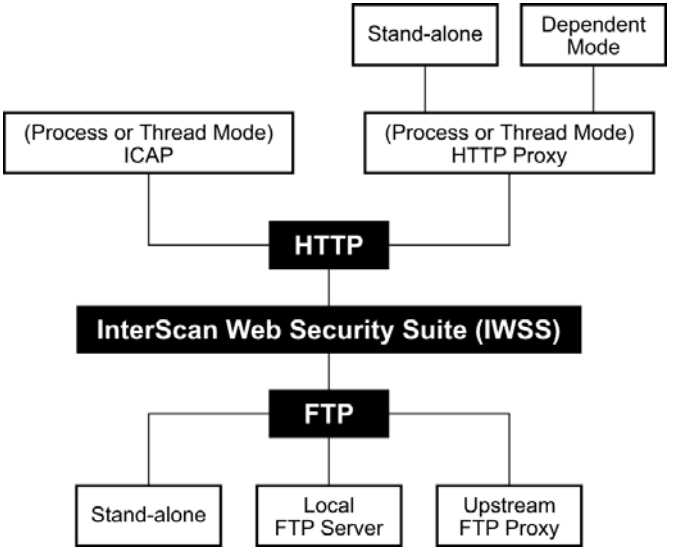


FIGURE 2-1. Possible installation options for HTTP proxy (stand-alone or dependent mode) and FTP (stand-alone, local FTP server, or upstream FTP proxy) in the IWSS console.

Recommended System Requirements

Install IWSS on a system with the following software and hardware:

- 512MB RAM (Add 1GB memory for URL filtering if URL filtering is installed)
- 150MB disk space (2GB if running the URL filter), plus 500MB for swap files)
- PC with an Intel Pentium™ IV 2.4GHz
- A monitor with 800x600 or greater resolution
- Active Directory Support - Windows 2000 server with Active Directory, or Windows 2003 server with Active Directory, SP1 recommended
- Microsoft™ Internet Explorer 5.5 with SP2, Internet Explorer 6.0. or Netscape™ Navigator 7.0 to access the IWSS Web console
- PostgreSQL 7.4.1 database (which is installed by default), also supports Oracle 8i/9i (Oracle support requires purchase of a third-party ODBC driver)
- ICAP 1.0-compliant cache server (not required for stand-alone mode)
  - NetApp™ NetCache™ release 5.6R1D6, or
  - Blue Coat Systems™ SGOS 2.1.10 and 3.1.2.2, or
  - Cisco™ ICAP servers (CE version 5.1.3, b15)

Platforms

- **Solaris**™ 2.8 or 2.9 on Sun™ Ultra SPARC™ II processor 550MHz
- **Linux**: Red Hat™ Advanced Linux Server 2.1, 3.0, or SUSE™ Linux Enterprise Server 9, or Red Hat Enterprise Linux (ES, AS) 3.0, Update 4

Note: (1) Install libstdc++ on the IWSS machine. If you are running Red Hat Advanced 3.0, the libstdc++ is available from www.redhat.com. If you are running SuSE Linux Enterprise Server 9, the libstdc++ library can be found in the "compat" package located on the IWSS installation CD.
(2) IWSS is a 32-bit application that can run on a 32-bit Intel Pentium processor-based Linux server.
(3) For multiple IWSS ICAP servers to work properly, their corresponding pattern, scan engine version, and `intscan.ini` files must be identical (see *Configuration Files* starting on page C-1 for more information). Also, these systems must share a database.
(4) Insufficient disk space may cause performance issues and/or errors.

HTTP Proxy Topology

IWSS provides a choice of either an ICAP or a stand-alone HTTP proxy protocol handler. The ICAP protocol handler enables IWSS to act as an ICAP server. When using the HTTP protocol handler, IWSS acts like a direct HTTP proxy server. If you are using the HTTP proxy, you can configure it to function in stand-alone mode (no upstream proxy) or in dependent mode (with upstream proxy).

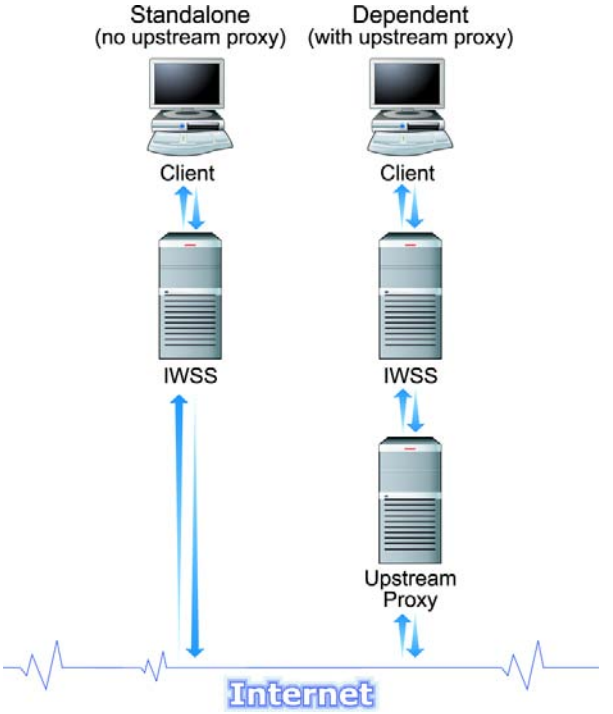


FIGURE 2-2. For dependent mode, type the proxy name and the port number in the IWSS console under "HTTP > Configuration > Proxy Scan".

Deploying HTTP in a Multiple Server Configuration

You can deploy HTTP in a multiple-server configuration. In this case, set up a database in a central location. See *Setting up the Database* starting on page 4-31 for more details. The configuration can be deployed in one of two ways:

- Multiple IWSS ICAP servers that work with a single ICAP client with load-balancing capability
- Multiple HTTP stand-alone servers that use a Layer 4 switch for load balancing

One IWSS server must be designated as “master” (see *Configuring Server Designation* starting on page 4-34 for more details). The configuration files (see *Configuration Files* starting on page C-1 for more details) must be synchronized manually, via Control Manager or via a customer-created script. You need a Layer 4 switch to load balance between IWSS servers for multiple HTTP stand-alone servers. However, for multiple ICAP servers, you need an ICAP client with a load balancing capability. To access the administrator console for each IWSS server, you can access the administrator user interface using the private IP addresses of each IWSS server.

IWSS HTTP Stand-alone Installation Topology with Multiple Servers

When IWSS is working in a multiple server configuration under a Layer 4 switch environment, IWSS distributes the list of infected URLs to all the IWSS servers in a multiple server configuration. The URL-blocking list for all IWSS servers in a multiple server configuration must be identical. When IWSS detects a virus originating from a particular URL, the URL is added to the URL-blocking list, which is maintained by the server itself. This particular proxy that has the most updated URL-blocking list submits the URL entries to the master server. The master server dynamically distributes the list to the other IWSS servers, except for itself and the source machine.

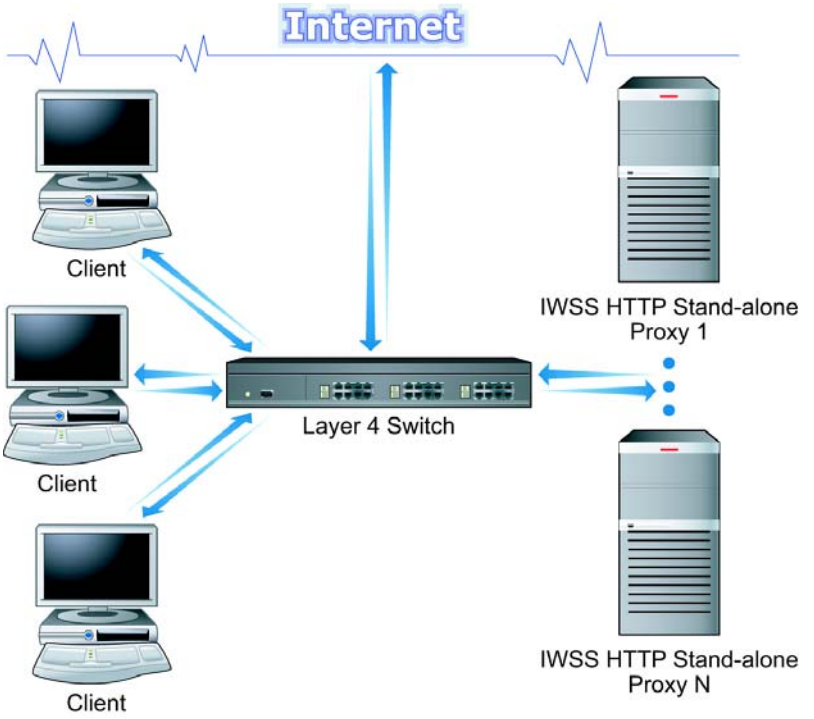


FIGURE 2-3. Use a Layer 4 switch to load balance between IWSS servers for multiple HTTP stand-alone servers.

IWSS ICAP Installation Topology with Multiple Servers

If there is already a content-cache server on your network, then ICAP is the logical choice; otherwise, use the HTTP proxy. The ICAP client can be a NetCache, Blue Coat Systems caching appliance, or Cisco CE ICAP server. The following diagram shows the installation topology for IWSS ICAP with multiple servers.

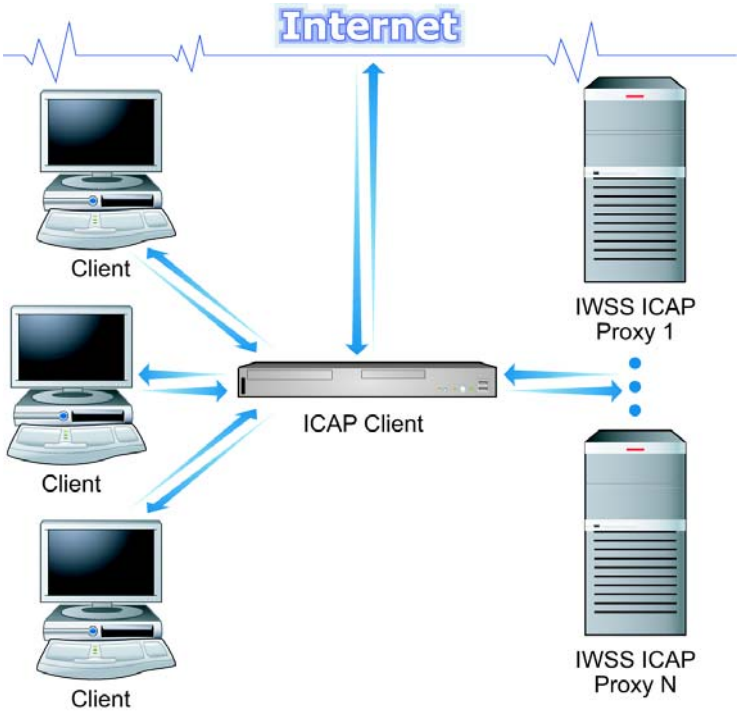
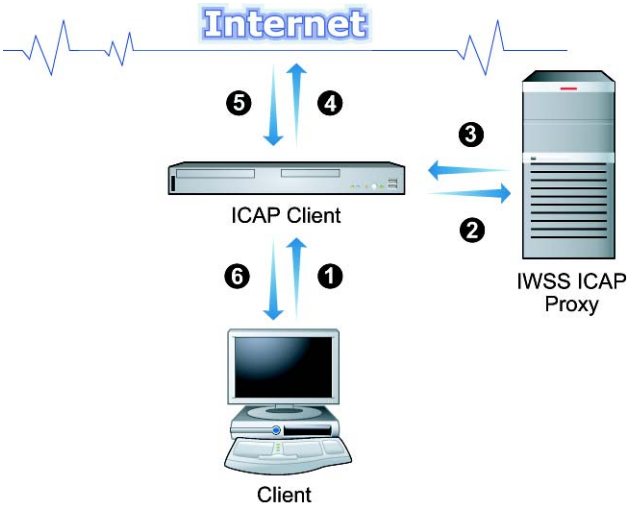


FIGURE 2-4. For multiple IWSS ICAP servers to work properly, their corresponding pattern, scan engine version, and intscan.ini files must be identical.

ICAP Request Mode Workflow

The IWSS ICAP request mode modifies the HTTP requests and is responsible for URL blocking and scanning uploads. The following steps describe the request mode workflow:

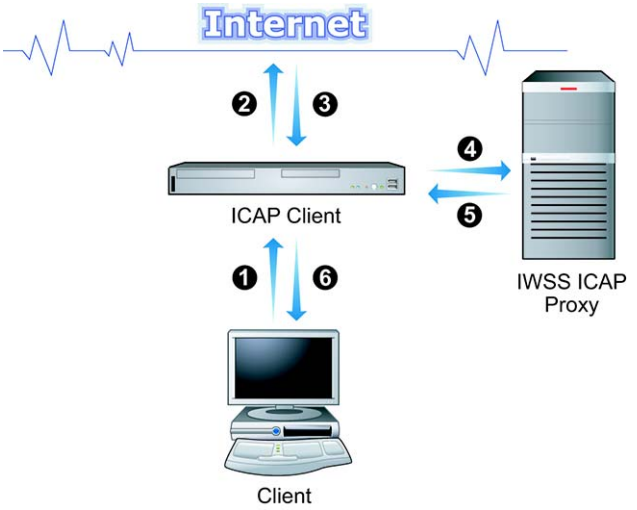
1. A Web client issues an HTTP request.
2. The ICAP client (content-cache servers) receives the request and directs it to the IWSS ICAP server.
3. The IWSS ICAP server takes the appropriate action (URL blocking or upload scanning) and forwards the request to the ICAP client.
4. The ICAP client sends the request to the Web server.
5. The Web server sends the response to the ICAP client.
6. The ICAP client forwards the response to the client.



ICAP Response Mode Workflow

The IWSS ICAP response mode modifies the HTTP response and is responsible for virus scanning. The following steps describe the response mode workflow:

1. A Web client issues an HTTP request.
2. The ICAP client sends the request to the Web server.
3. The Web server sends the response to the ICAP client.
4. The ICAP client sends the response to the IWSS ICAP server.
5. The IWSS ICAP server modifies the response depending on the setting (for example, virus scanning) then sends it back to the ICAP client.
6. The ICAP client forwards the response to the client.



FTP Installation Topology

There are three configuration topologies for FTP:

- Stand-alone mode acts as a proxy between the requesting client and the remote site, brokering all transactions
- IWSS FTP acts in conjunction with an existing FTP proxy within the LAN
- IWSS FTP acts as a sentry standing guard for the local FTP server

Stand-alone Mode

If you want to scan all FTP traffic in and out of the LAN, set up FTP so that it "brokers" all such connections. In this case, clients FTP to IWSS FTP, supply the logon credentials to the target site, and then let IWSS FTP make the connection. The remote site transfers the files to IWSS FTP. Before delivering the files to the requesting clients, IWSS FTP scans these files for viruses.

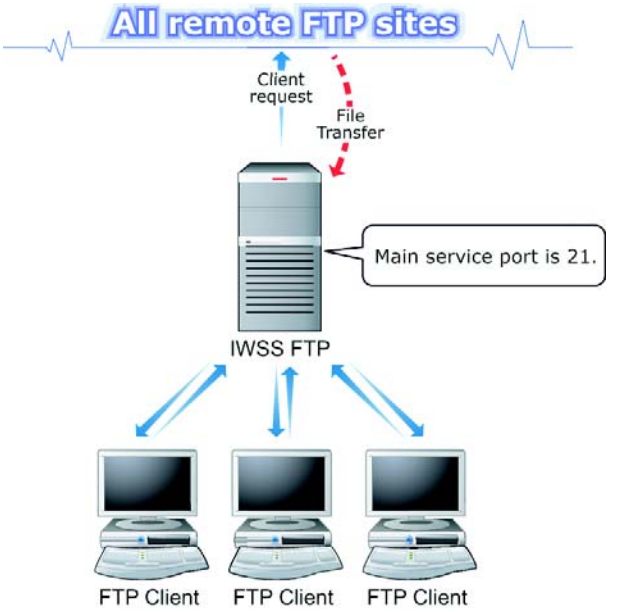


FIGURE 2-5. Configure the FTP proxy setting in the IWSS console.

Local FTP server

If you want to scan all FTP traffic in or out of a particular FTP server (typically one that you host), you can install IWSS FTP onto that FTP server (as one local server). In this case, it appears to users that they are connecting directly to the target server when in fact they are connecting to IWSS FTP, which then relays the request to the specified server.

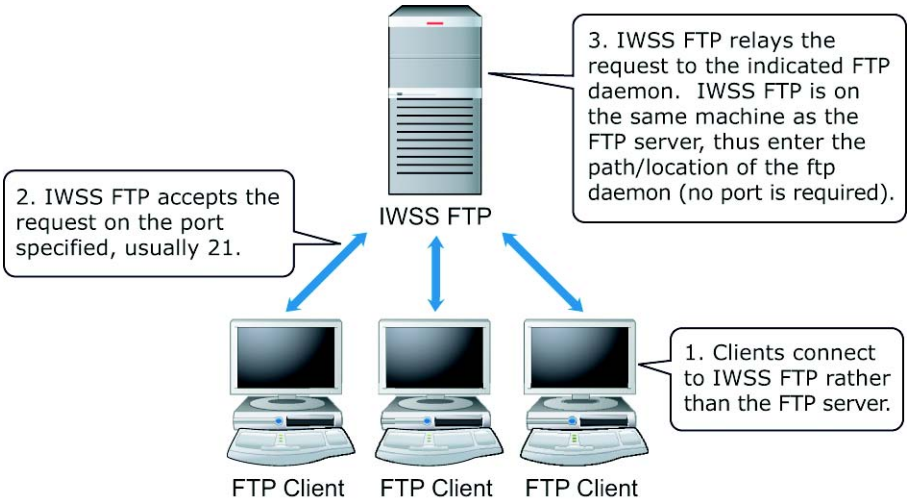


FIGURE 2-6. For Local FTP server, indicate the new direction of the path (for example, /usr/sbin/in.ftpd).

Upstream FTP Proxy

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

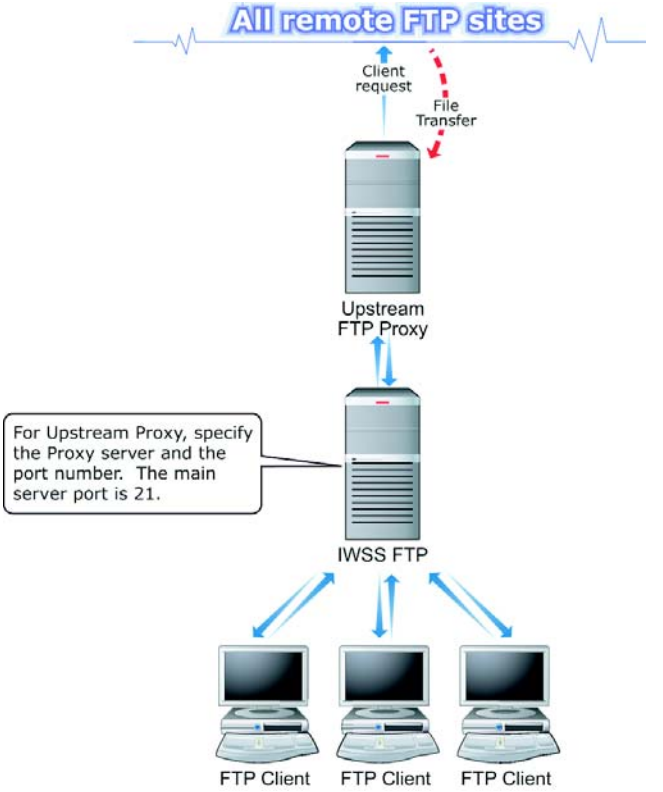


FIGURE 2-7. Using IWSS with an upstream FTP proxy

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

Report and Database Setup

IWSS provides you with 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 a specific user, 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).

There are two categories of reports:

- Blocking-event reports
- Traffic reports for URL filtering

You can view the following report types for each category on the IWSS console:

Blocking-event Reports

- Riskiest URLs by viruses detected
- Riskiest users by infected URLs accessed
- Most violations by user
- Most violations by group
- Most blocked URL categories
- Most blocked URLs
- Most blocked URLs by day of the week
- Most blocked URLs by hour

Traffic Reports

- Most active users
- Most popular URLs
- Most popular downloads
- Most popular search engines
- Daily traffic report
- Activity level by day of the week

- Activity level by hour
- Per user report

Note: Traffic reports require that the access log be enabled. However, the trade-off is that the access log can be very large.

Spyware/Grayware Reports

- Most spyware/grayware detections by category
- Top spyware/grayware detections
- Most detections by user

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 IWSS 1.0 and to further analyze the log data using custom scripts or other third-party applications. They can also be used in validating the completeness and accuracy of logging to the database.

Trend Micro recommends that you migrate to "database only." Data for reports is recorded to the database at a configurable interval. Reports and database logs will not reflect the activity, which has occurred after 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 not enabled. Conversely, if IWSS is configured as an upstream proxy, valuable data on user activities may not be available to IWSS. Thus, you need to decide whether or not you want IWSS to be the mechanism to summarize all Web activities. If you do, then access logging must be enabled under **Logs > Settings > Reporting Logs > Options**.

The IWSS Web console displays the graphs (Bar, Stacked bar, or Line) and statistics of a generated report. In addition, you can import data from IWSS logs for further analysis using Microsoft Excel (see *Importing Data* starting on page 8-20 for more details). In order to query and generate reports dynamically, IWSS uses an efficient database management system that can support other major databases as a plug-in. The IWSS package includes the PostgreSQL 7.4.1 database. IWSS also supports Oracle 8i/9i. See *Important Notes on Oracle 8i/9i Database* starting on page 3-7 and

Important Notes on PostgreSQL Database starting on page 3-10 for more information on database installation and configuration.

User Identification Process

IWSS helps to trace security events to the affected systems. IWSS includes three event-tracing mechanisms.

- Identify by the IP address
- Identify by the host name (modified HTTP headers)
- Identify by the user/group name via proxy authorization (use LDAP for account information)

This choice controls the information that IWSS includes in the virus log, Internet access log, and URL blocking and filtering logs. IWSS URL filtering also uses this information for policy management.

Tracing security events to the affected system is important because IWSS scans for malicious code that is uploaded using HTTP. When you detect an upload that contains malicious code, the originating system is infected. In addition, if you are using "scan-behind" (see *Handling Large Files* starting on page 4-5 for details), a large file that contains malicious code may have been delivered to a client system and subsequently determined to be malicious. If the affected client does not have sufficient protection, you may need to find the affected client and perform a cleanup. Tracing a virus from the virus log may be useful when tracing these types of suspicious behavior.

The **IP address** identification option requires that IP addresses are not dynamically assigned via 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.

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. The program **register_user_agent_header.exe** is in the Linux/Solaris installation package. An effective way to deploy 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 **User/group name via proxy authorization (use LDAP for account information)** option verifies the user credentials as well as retrieves the group information. IWSS uses LDAP to integrate with Active Directory, as a network service that identifies all resources on a network and makes them accessible to users and applications. This 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 utilize 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 authentication)

If you are using Microsoft Internet Explorer, IWSS uses the NTLM authentication protocol to verify your credential with the Active Directory. NTLM employs a challenge-response mechanism for authentication, in which clients are able to prove their identities without sending a password to the server. Internet Explorer uses the single sign-on mechanism while using NTLM at the first pass so that you will not be prompted for your credential; however, if the verification fails, a dialog box will prompt to check your credentials. For other browsers, a basic authentication is used. In this case, you are prompted for your credential and the user name and password are encoded using the Base64 encoding method, which is not a secure practice.

Note: You can only configure one LDAP (AD) server to authenticate user/groups information for one particular domain.

Notes on User/Group Name via Proxy Authorization

User/group proxy authorization as a technique for user identification resolves some of the limitations of the following 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 originated
- Host name (modified HTTP headers): This approach solves the problems with using IP address, but works only under Windows and only for Internet access 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

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

Proxy authorization is the most accurate and flexible user identification method. The use of proxy authorization is transparent for Internet Explorer users. Trend Micro recommends that proxy authorization be used so long as a network path between IWSS and the Active Directory server can be established, and the inconveniences described below can be tolerated.

Proxy authorization has some drawbacks that must be considered, and these apply to other browsers and HTTP-based applications. The primary drawback is *inconvenience* for the end user. IWSS requires that incoming requests authenticate by providing the user's user name and password on a pop-up dialog box. 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 to other applications,

including any additional instances of the same application. As a result, the user may have to answer the challenge 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 NTLM authentication techniques when installed in HTTP proxy mode, but only Basic when installed in ICAP mode.

You also need to plan on how to manage users who do not have an account in the local domain. For example, a vendor may need to give a demonstration that requires Internet access. In a normal office setting, the IT department can set up two proxies: one for users with accounts (with the domain logon script configured so that their browsers can use that proxy), and the other proxy for visitor use. Both proxies could be instances of IWSS with different configurations.

In network environments where IP addresses adequately identify the machines where requests originate, IWSS can utilize a cache that assumes that for some time after the user from a particular IP has been authenticated, any additional requests from that same IP are issued by the same user. The default time-to-live (TTL) for entries in this cache is 12 minutes in HTTP mode and 90 minutes in ICAP mode.

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

Consider the following:

TABLE 2-1. 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 require a popup and the user must 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 Mozilla	

Chapter 3

Installation and Setup

In this chapter, you will find step-by-step instructions for installing and configuring IWSS. Topics included in this chapter are:

- Process Mode and Thread Mode
- Installing InterScan Web Security Suite
  - HTTP stand-alone proxy server
  - ICAP-compliant cache server
- Opening the IWSS Console
- Encrypting Browser-console Communication (HTTPS)
- Testing IWSS
- Updating the Virus Pattern File
- Updating the PhishTrap Pattern File
- Updating the Spyware Pattern File
- Updating the URL Database (for URL Filtering Option Only)
- Updating the Scan Engine
- Activating IWSS and URL Filtering
- Renewing Your Maintenance Agreement
- Removing IWSS
- Upgrading IWSS

Process Mode

In *Process* mode, the daemon runs as a parent process with many child processes. The parent manages the life span of all of the child processes, while each child process handles one connection to the server for the lifetime of that connection. As traffic subsides and child processes become idle, the parent removes the extra idle processes and keeps only a minimum number of child processes to wait for traffic.

- The primary advantage of this model is 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.
- Another advantage is that because each child process has little communication with either its parent or other child processes, there is very little communication overhead, which translates to greater throughput, in cases where network latency is low.
- The primary disadvantage is that each connection requires a whole child process, and each process has a significant memory footprint (about 24MB), which can limit the maximum number of child processes that can be spawned, and therefore limit the maximum number of concurrent connections.

Thread Mode

In *Thread* mode, the daemon runs as one process that contains several threads (similar to processes that share the same memory space). The worker threads handle the connections. The number of worker threads remains constant until you modify it, and each thread can handle many simultaneous connections.

- The primary advantage of thread mode is that, even with hundreds of connections open, the daemon has a small footprint, typically between 200-500MB (virtual memory). The CPU, not the number of worker threads or memory, limits the number of connections that the threaded daemon can handle.

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

- Another advantage to thread mode is that 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.

- The primary disadvantage of the thread mode is that all the threads occupy the same process space; therefore, if a programming fault causes one thread to crash it will stop the daemon.
- Another disadvantage is that, due to the need to synchronize access to shared memory, some computations require more overhead than in the process mode. This can result in lower throughput when network latency is low.

Tuning Solaris for IWSS

IWSS uses the standard UNIX System V IPC semaphores to synchronize log file access between processes. When running the multi-process mode IWSS daemon, it is necessary to increase the number of semaphores undo structures (represented by SEMMNU) configured on the system. If you do not perform this modification and you have a busy system (that is, the number of concurrent connections is more than the default value for the number of semaphores undo structures), then some connections will stop writing log entries to the Control Manager console and local system log, and an error message appears in the IWSS Web console. Perform this procedure (recommended before installation) only for process-mode installs and not for thread mode installs unless the same machine is running with other semaphore intensive applications (for example, database).

To increase the number of semaphores undo structures configured on the system:

1. Calculate the number of undo structures needed as follows. Examine the maximum number of IWSS scanning processes allowed, which is the lesser of the maximum number of users expected to be browsing the Web simultaneously and the virtual memory system divided by 70MB. After the installation, you can determine the maximum number of processes, which is stored in `[process]/max_proc` in `intscan.ini`. Add the maximum number of FTP scanning processes (this value is also stored in `[ftp]/max_proc` in `intscan.ini` after installation) if you install FTP scanning. Then, multiply the total number of maximum processes by 5, and add the current value of SEMMNU; obtain the SEMMNU value by typing the following command:

   ```
   sysdef | grep -i semmnu
   ```

The formula for semmnu is:

Old semmnu + (<http max_proc> + <ftp max_proc>) * 5

If URL filtering is enabled, add <`http max_proc`>.

For example,

If you install IWSS in multi-process mode with `max_proc` set to 200, and then you install FTP scanning daemon with `max_proc` set to 1, and the current value of SEMMNU is the Solaris default of 30.

Then new semmnu value should be at least:

(201 * 5) + 30 = 1035

If you also add URL filtering, then this should be

(201 * 5) + 30 + 200 = 1235

2. Edit the `/etc/system` file and add the line:

set semsys: `seminfo_semmnu = X`

where X is the value computed in step 1

3. Reboot the system.

Installing InterScan Web Security Suite

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

Note: An Activation Code is required to enable scanning and product updates (see *Activating IWSS and URL Filtering* starting on page 3-41 for more information).

To install InterScan Web Security Suite:

1. You can install IWSS from the Trend Micro Enterprise Solutions CD or download the installation files from the Web.

To install from the Trend Micro Enterprise Solutions CD:

Insert the CD-ROM disc into the CD-ROM drive of the server where you will install IWSS. Choose **InterScan Web Security Suite** from the **Choose a product** drop-down menu and click **Go**. Then, run the install script from the product folder on the Enterprise Solutions CD.

To download an evaluation version:

If you are downloading from the Web, download the IWSS binary archive to a temporary directory on the server where you want IWSS to run, and then extract the files.

2. From the directory containing the IWSS installation files, type `./isinst` and press **Enter**.
3. The **IWSS 2.2 Setup Script** page appears with the following install options:
   - InterScan Web Security Suite HTTP scanning
   - InterScan Web Security Suite FTP scanning
   - InterScan Web Security Suite URL filtering

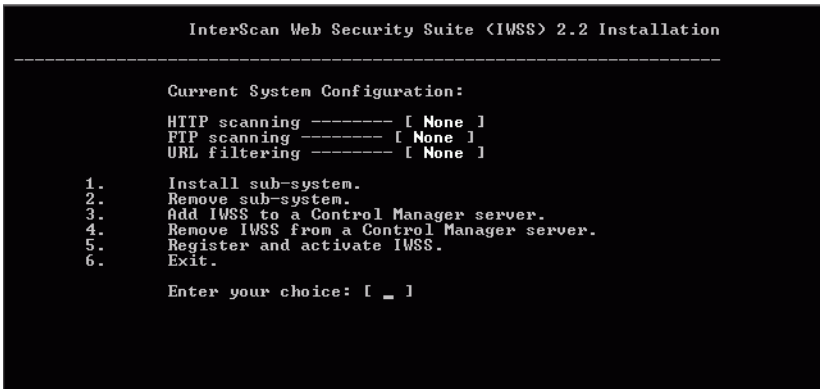


FIGURE 3-1. "URL Filtering" requires a separate Activation Code to be functional.

4. Type **1** and press **Enter** to install **InterScan Web Security Suite sub-system**. The **Trend Micro License Agreement** page appears. Press **Enter** to continue viewing the agreement. Type **Y** to accept the license agreement or type **N** to deny the agreement (this will discontinue the installation process). When you

accept the license agreement, the **InterScan Web Security Suite Installation List** page appears.

5. Type **5** and press **Enter** to start the installation.

Note: By default, IWSS installs all available sub-systems to the `/opt/trend/IWSS` subdirectory. If you want to install to a different directory, type **4** and type the new path under **New Path is** and press **Enter**. Selecting one of the modified options from **1** to **3** allows you to choose the components to be installed or uninstalled. After each selection is made, a separate prompt appears to allow you to enter "y" (yes) and "n" (no) to install the selected component. Also, the URL filtering component is dependent on the HTTP scanning component; therefore, in order to install the URL Filtering component the HTTP component must be installed (either previously, or installed simultaneously with the URL filtering component).

---

6. On the next screen, type **Y** to install the default PostgreSQL database, otherwise type **N**. You can use Oracle 8i/9i but you need to install it separately (see *Important Notes on Oracle 8i/9i Database* starting on page 3-7 and *Important Notes on PostgreSQL Database* starting on page 3-10 for more information on installation and configuration).
7. Type and confirm the password for the database administrator. Press **Enter** to continue.
8. On the next screen, choose the type of HTTP handler. Type **1** for ICAP and **2** for HTTP Proxy (see *Protocol Handlers* starting on page C-2 for more information).
9. Specify the mode (Process or Thread) and press **Enter** to continue. Type **1** for Process mode or **2** for Thread mode.

Note: Thread mode is recommended for smaller networks that service a low bandwidth Internet link. Process mode is recommended for larger networks that serve high capacity Internet links.

---

10. The Control Manager agent for IWSS is installed by default. Press **Enter** to continue. From the main menu, type **3** to register the Control Manager agent with a designated Control Manager. See *Trend Micro Control Manager* starting on page 9-1 for more information.

11. Once the installation is complete, you will return to the main menu. Type **5** and press **Enter** to activate IWSS.
12. In the next page, specify the browser you will use (for example, `netscape`). Type the logon User ID and password if prompted (default value: **admin**).
13. In the **Product License** page, activate IWSS by typing your Activation Code in the field provided and click **Activate**.

> **Note:** If you do not activate IWSS, security updates and scanning capabilities will not be functional. You can also activate IWSS using the IWSS console.

14. Type **6** and press **Enter** to exit the script.

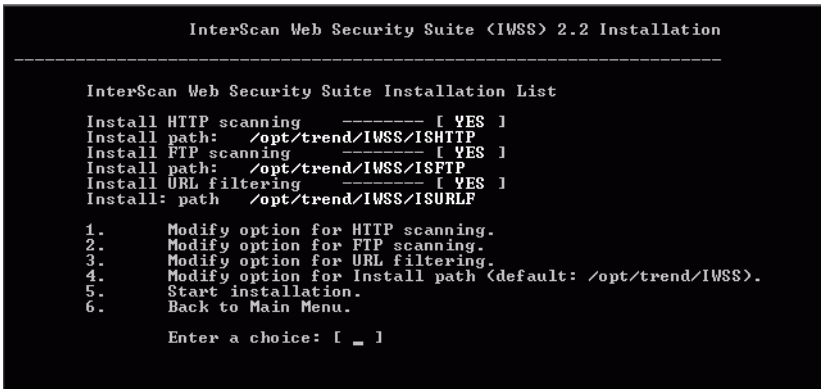


FIGURE 3-2. Type "1" to modify IWSS HTTP; "2" to modify IWSS FTP; "3" to modify IWSS URL Filtering; and "4" to modify the installation path.

Important Notes on Oracle 8i/9i Database

To create an Oracle database:

The Oracle Server 8i/9i must be installed on a remote machine or on the same machine where the IWSS server resides.

1. Create a database using UTF 8 character set.
2. Create a user (for example, username: "IWSS" and password: "IWSSpassword") for the new database to be used for IWSS (for example, "IWSSDB" is used as the

Oracle database service name/global database name for Oracle 8i and higher) with the following permissions:

- Create tables
- Store and execute procedures
- Grant the roles “CONNECT” and “RESOURCE” to the new database user.

For example,

Create a user with [Profile: Default] [Tablespaces “users,” “Temporary: TEMP”] [Granted Role: CONNECT and RESOURCE] [System: UNLIMITED TABLESPACE]

To configure the Oracle Client 8i/9i on the same machine where IWSS resides:

Install the Oracle client on the same machine where IWSS is installed. Configure the Oracle client so that it can communicate with the Oracle server with a valid database connection string. The goal is to create a connection string for IWSS to communicate with the Oracle server. The steps mentioned below describe the procedure to use an Oracle client configuration assistance to configure a connection string to be used by IWSS to connect to the Oracle server.

1. Start the Oracle client configuration assistance by typing `netca`.
2. On the next screen, select **Local Net Service Name configuration**. Click **Next**.
3. Select **Add** for the new Oracle service name.
4. Select **Oracle8i or later database service**.
5. Enter a new service name/global database name under the **Service Name** field.
6. Select **TCP** as the protocol for Oracle Client / Server communication.
7. Enter the Oracle server hostname and type a port number (the default is 1521).
8. Select **Yes, perform a test**.

Note: If the test fails, click **Change Login** to change to a different DBA account, and then type the user account and password.

---

9. Click **Next**.

To test the Oracle Client/Server communication:

1. Type `sqlplus /nolog`.
2. In the next screen, type the following:

```
SQL> connect <username>/<password>@<database service name>
For example,
SQL> connect IWSS/IWSSpassword@IWSSDB
```

To install unixODBC:

Install unixODBC for 32-bit SPARC Solaris / x86 Linux on a machine where IWSS resides. The unixODBC requires separate licenses for Solaris and Linux platforms.

To populate the Oracle database:

Populate the IWSS schema in the Oracle database by performing the following:

1. Run `setup-oracle-env.sh` in the installation package to create the database schema on the Oracle server.
2. Specify the [ORACLE_HOME] path where the Oracle Client was installed.
3. Specify the Net service name (connection string) for the Oracle database.
4. Enter the user name and password for the Oracle database.

Note: The `setup-oracle-env.sh` script uses the value (as the default path) defined in ORACLE_HOME, where the Oracle client was installed, unless otherwise specified. The `setup-oracle-env.sh` script tests the connection between unixODBC with the Oracle client and the Oracle client with the Oracle server. IWSS should be installed prior to running `setup-oracle-env.sh`.

To remove the IWSS schemas from the Oracle database server (remote/local):

1. Run the `cleanup-oracle-env.sh` script from the IWSS installation package.
2. Specify the [ORACLE_HOME] path where the Oracle Client was installed.
3. Specify the Net service name (connection string) for the Oracle database.
4. Enter the user name and password for the Oracle database.
5. Select **y** to remove all tables and stored functions related to IWSS.

Note: IWSS should be installed prior to running `cleanup-oracle-env.sh`. The `cleanup-oracle-env.sh` script uses the value (as the default path) defined in ORACLE_HOME, where the Oracle client was installed, unless otherwise specified.

Important Notes on PostgreSQL Database

To manually install the local PostgreSQL database provided from the IWSS installation package:

1. After installing IWSS, run the `installdb.sh` script from the installation package. Enter the user name and password for the PostgreSQL 7.4.1 database.
2. Run the `setup-postgres-env.sh` script from the installation package.
   a. Type the PostgreSQL server name/IP address of the local machine (the default value is `localhost`.
      - use the default port [5432].
      - use the default database name [iwss].
      - use the default user name for the PostgreSQL [sa].
   b. Type the database password entered when running the `installdb.sh script`.
   c. Choose whether to create the tables on the PostgreSQL database.

Note: Make sure that you run the `installdb.sh` script after installing IWSS.

To manually remove the locally installed PostgreSQL server provided from the IWSS installation package:

Run the `uninstalldb.sh` script from the installation package. Make sure that you run the `uninstalldb.sh` script where IWSS is installed. When the PostgreSQL server has been successfully removed, the `PostgreSQL removed` message appears.

To use an existing PostgreSQL database server (remote/local):

1. Run the `setup-postgres-env.sh` script from the installation package.
2. Type the following information:

- PostgreSQL server name / IP
- database name of the PostgreSQL server
- user name and password for the PostgreSQL database

3. Choose whether to create tables on the PostgreSQL database.

Note: IWSS should be installed prior to running `setup-postgres-env.sh`. For the pre-existing PostgreSQL server configuration, a pre-existing database needs to be present prior to the running the `setup-postgres-env.sh script`.

To remove the IWSS schema from the PostgreSQL database server (remote/local):

1. Run the `cleanup-postgres-env.sh` script from the installation package.
2. Type the following information:
   - PostgreSQL server name / IP
   - PostgreSQL port number
   - PostgreSQL database name
   - User name and password for the PostgreSQL database

Note: IWSS should be installed prior to running `cleanup-postgres-env.sh`.

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 IWSS Console* starting on page 3-20.

After installing the IWSS ICAP program files,

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

1. Setting up an ICAP 1.0-compliant Cache Server

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

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.

To 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**.

4. 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**.
5. 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.

6. Under the **Consistency** field, choose **strong** from the drop-down menu and leave the **lbw Threshold** field empty.
7. 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 (see *Configuration Files* starting on page C-1) and the same virus pattern. The service farm will not work properly if the ICAP servers have different configurations.

8. 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 **Access Control List**, and then add “icap (service farm name)” any into the **FTP ACL** field.

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**.

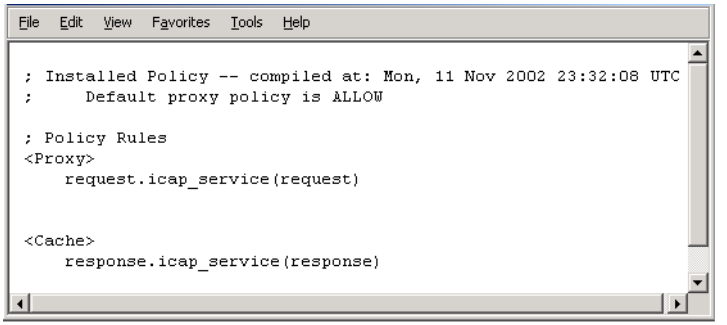


FIGURE 3-3. Configure both the request and response mode ICAP services. To check the current policy, go to the "Policy" screen, click the "Policy Files" tab, and then click "Current Policy".

To set up 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. Type `?` to display a list of all available commands. Type the following commands:

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

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

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

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

   ```
   icap service REQUESTMOD SERVICE NAME
   ```

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

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

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

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

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

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

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

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

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

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

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

Configuring Virus-scanning Server Clusters

For the Blue Coat Port 80 Security Appliance to work with multiple virus-scanning servers, 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.

2. Flushing Existing Cached Content from the Appliance

There is a potential threat of infection from content cached to the NetCache appliance, Blue Coat Port 80 Security Appliance, or the Cisco ICAP servers before IWSS ICAP started scanning HTTP traffic. Trend Micro recommends that you flush the cache immediately after installing IWSS ICAP. All new requests for Web content will then be served from the Internet and scanned by IWSS ICAP before caching. Scanned content is then cached on the NetCache appliance, Blue Coat Port 80 Security Appliance, or the Cisco ICAP servers. The NetCache appliance, the Blue Coat Port 80 Security Appliance, or the Cisco ICAP servers will serve future requests for the same Web content by your network users. Since the request is not sent to the Internet, download time is accelerated.

To flush the cache in NetCache:

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

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

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

To flush the cache in the Cisco ICAP server:

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

Opening the IWSS Console

Trend Micro recommends opening the IWSS console and modifying the default configuration to match your organization's security policies.

Remote configuration is also possible. Open a Web browser, and then type the IWSS URL followed by the port number **1812**. The URL can be typed using the qualified domain name, machine name, or IP address of the IWSS machine. For example,

```
http://domain:port/index.jsp
http://<machinename>:1812/index.jsp
http://123.123.123.12:1812/index.jsp
```

See *Accessing the IWSS Console via HTTPS* starting on page 3-22 for information on how to access the IWSS console via HTTPS.

Password Management

Your 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.

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 mis-spell words
- Use phrases or combine words
- Use both uppercase and lowercase letters

To change the console password:

1. Open the IWSS console and click **Administration > Password** in the left menu.
2. Type your current password in the **Old password** field, and then type and confirm the new password you want to use.

3. Click **Save** to save your new password.

FIGURE 3-4. Use a password (password is case-sensitive) that is difficult to guess with 4-32 (preferably at least 8) 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/ISADMIN/IScan.adm/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 prompts and use `iwss20` (for this example) as the password.

   The file `mykeystore` is generated in the current working directory.

3. Copy `mykeystore` to the Tomcat base directory. (`/opt/trend/IWSS/ISADMIN/IScan.adm/AdminUI/tomcat`) or to the set base directory in the `CATALINA_HOME` environment variable.
4. Copy and insert the following block under the **<Service name="Tomcat-Standalone">** section in the `server.xml` file located in the following file:
   `/opt/trend/IWSS/ISADMIN/IScan.adm/AdminUI/tomcat/conf/server.xml`

```
<Connector
className="org.apache.catalina.connector.http.HttpConnector"

   port="8443" minProcessors="5" maxProcessors="75"

   enableLookups="true"

   acceptCount="10" debug="0" scheme="https"
   secure="true">

   <Factory
   className="org.apache.catalina.net.SSLServerSocketFactory"

   clientAuth="false" protocol="TLS"
   keystoreFile="mykeystore" keystorePass="iwss20"/>

   </Connector>
```

Note: Include the `keystoreFile` and `keystorePass` parameters if you are not using the default keystore name or the default Tomcat keystore password `changeit`.

5. 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 the 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

To protect the communication between the IWSS server and the browser, disable non-HTTPS access.

To disable non-HTTPS access:

1. Edit the Tomcat http configuration file `/opt/trend/IWSS/ISADMIN/IScan.adm/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="20000"

               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

Testing IWSS

After installing IWSS, test the following to verify that IWSS is working properly. There are five types of test to perform:

- Testing upload scanning
- Testing FTP scanning
- Testing URL blocking
- Testing download scanning
- Testing URL filtering
- Testing spyware scanning
- Testing PhishTrap

EICAR test file

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 whose 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.

Note: Never use real viruses to test your antivirus installation.

Obtaining the EICAR Test File

You can 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 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.

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 > Scanning** in the left menu. Clear **Enable HTTP 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 > Scanning** in the left menu, select **Enable HTTP scanning**, and then click **Save**.
5. Send a mail with one of the test viruses as an attachment by using any Internet mail service.

FIGURE 3-5. This warning screen shows the detection of an EICAR test virus.

Testing FTP Scanning

The following procedure contains end-user instructions on how to test FTP virus scanning. See *FTP Installation Topology* starting on page 2-13 for more information about FTP installation topologies.

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 console 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 the message shown in the figure below.

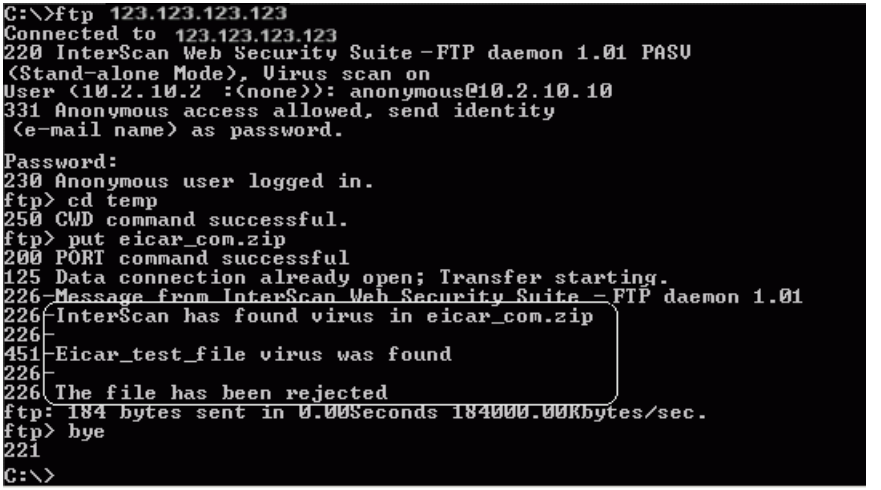


FIGURE 3-6. This is a warning message that shows the detection of a virus in eicar_com.zip.

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.

For more information about the HTTP topology, see *HTTP Proxy Topology* starting on page 2-7.

To test URL blocking:

1. Open the IWSS console and click **HTTP > URL Blocking** in the left 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.

FIGURE 3-7. A sample warning message for a blocked URL site.

Testing Download Scanning

To test virus scanning when downloading using HTTP or FTP over HTTP, select a test virus on the following Web site:

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

FIGURE 3-8. The following virus-warning screen appears if the system is set up properly.

If a user attempts to download an infected file, IWSS will block other users' access to that site for four hours by default. When subsequent users 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` (see *Configuration Files* starting on page C-1 for more information).

Testing URL Filtering

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

1. Open the IWSS console and click **HTTP > URL Filtering Policies** in the left menu. Select **Enable URL filtering**, which is available on four of the following screens: **Global**, **Policy List**, **URL Categories** and **Schedule**.
2. In the **URL Filtering Global Policies** screen, the "Company Prohibited Sites" in the **URL Category** column is blocked during work and leisure by default.

   Open a browser and access any site (for this example, www.urlfilteredsite.com), which is categorized in "Company Prohibited Sites."

FIGURE 3-9. The following message appears if the URL filtering system is set up properly.

Testing Spyware Scanning

Perform the following procedure to test for spyware scanning.

1. Open the IWSS console and click **HTTP > Scanning > Spyware/Grayware Scan Rule** in the left menu.
2. Enable spyware and other grayware categories for scanning.
3. Click **HTTP > Scanning > Action** in the left menu
4. Under the **Uncleanable files** field, select the action setting (Delete, Quarantine, or Pass).

5. Click **Save**.
6. After a successful spyware detection, a sample message appears:

FIGURE 3-10. A sample message after detecting a spyware with action "Delete" setting.

Testing PhishTrap

Perform the following procedure to test PhishTrap.

1. Open the IWSS console and click **HTTP > URL Blocking > Via Pattern File (PhishTrap)**.
2. Select **Enable URL blocking**.
3. Under **Block the following PhishTrap categories**, select all four categories (Phishing, Spyware, Virus accomplice, Disease vector).
4. Click **Save**.
5. After a successful phishing site detection, a sample message appears:

FIGURE 3-11. A sample message after detecting a phishing site.

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 (see *About ActiveUpdate* starting on page 1-15 for details) 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 weekly. 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 (see *About ActiveUpdate* starting on page 1-15 for more details).

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 and PhishTrap Pattern Update Schedule** section, select from the following options:
   - Minutes
   - 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** 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.

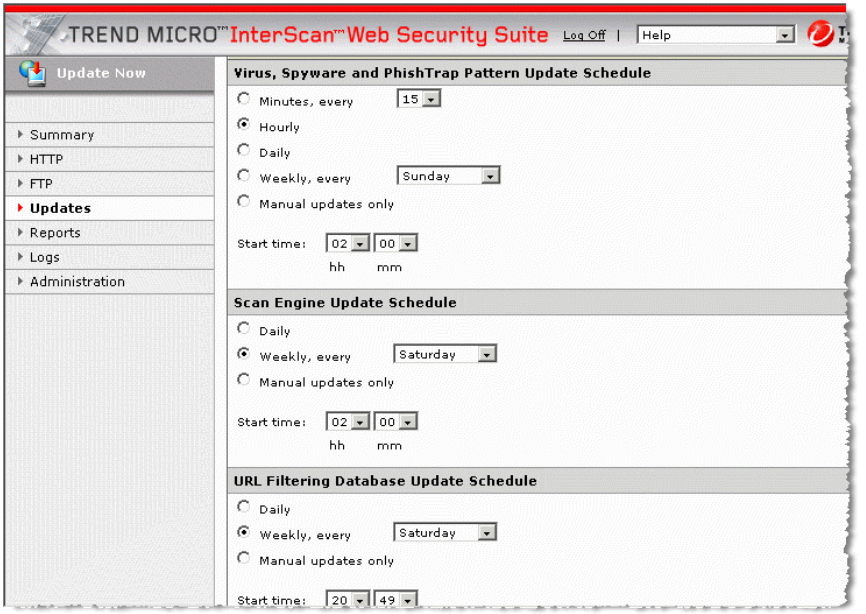


FIGURE 3-12. Automatically scheduled virus pattern, spyware, PhishTrap, URL filtering database, and scan engine updates can be configured via the IWSS console.

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 `/opt/trend/IWSS/ISBASE/IScan.BASE`. 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 **PhishTrap 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.

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 `/opt/trend/IWSS/ISBASE/IScan.BASE`, uses the following naming format:

```
tmaptn.###
```

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

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

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

To manually update the spyware pattern file:

1. Open the IWSS console and click **Summary** in the left menu.
2. Select **Spyware pattern** under the **Component** column and click **Update**. A progress bar indicates 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 (see *About the Trend Micro Scan Engine* starting on page 1-18 for more details).

To manually update the scan engine:

1. Open the IWSS console and click **Summary** in the left menu.
2. Select **Scan engine** under the **Component** column and click **Update**. A progress bar indicates 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 (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 database 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 **URL filtering database** under the **Component** column and click **Update**. A progress bar indicates 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 Update Schedule** section, select from the following options:
   - Daily
   - Weekly (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**.

Rollback Option

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, or virus pattern file:

1. Open the IWSS console and click **Summary** in the left menu.
2. 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.

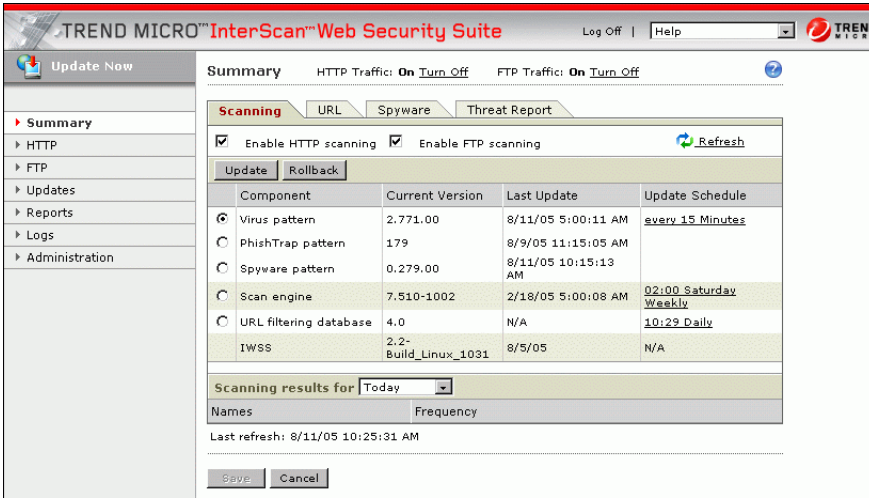


FIGURE 3-13. You can only perform a virus pattern, PhishTrap pattern, spyware pattern, and scan engine version rollback to one version lower than your existing current version.

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. 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.
3. 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 > 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**.

FIGURE 3-14. 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 > Notification**.
2. Select from the three options if the updates are:
   - Successful
   - Unsuccessful
   - Not needed
3. You can configure the email settings by clicking  on the **Notification** screen. Type a value for each of the following configuration fields:
   - Email address of the receiver of the notification messages in the **To address(es)** 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(es)** field

- Domain name or the IP address of the mail server that will send the notification messages in the **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 **Check mail queue in minutes** field.

4. Click **Save**.

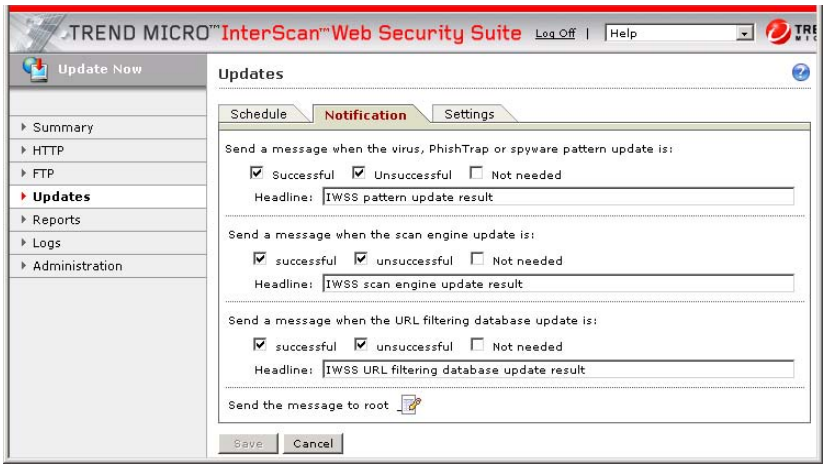


FIGURE 3-15. You can also configure the notification settings in the "Updates > Notifications" screen.

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 **Product License** screen, you can obtain an Activation Code online, view renewal instructions, and verify the status of your product.

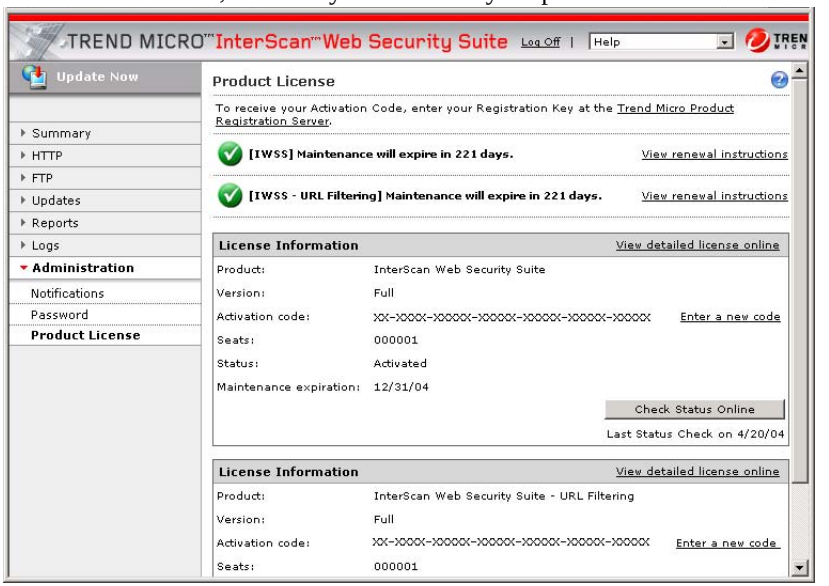


FIGURE 3-16. In the "Product License" screen, click "Enter a new code" to upgrade from evaluation to full version.

To obtain an Activation Code online:

1. Open the IWSS console and click **Administration > Product License**.
2. Click **register online**.
   For new customer registrations, click **Register your product**.
   a. 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.
   b. 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**.

c. The **Confirm Registration Information** screen appears. Click **Edit** to update your contact information and click **OK** to continue.

d. The **Activation Code** screen appears. The system informs you that your Activation Code will be sent to your registered email address.

e. Click **OK**.

For existing registered users, type your logon ID and password in the fields provided, and then click **Login**.

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

a. The **My Products** screen appears. Click **Add Products** and type the Registration Key. To edit your company profile, click **View/Edit Company Profile**.

b. Your Activation Code appears on the next screen. To receive a copy of your Activation Code through your registered email address, click **Send Now**.

3. 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.

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: The Maintenance Agreement expires. Your License Agreement does 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.

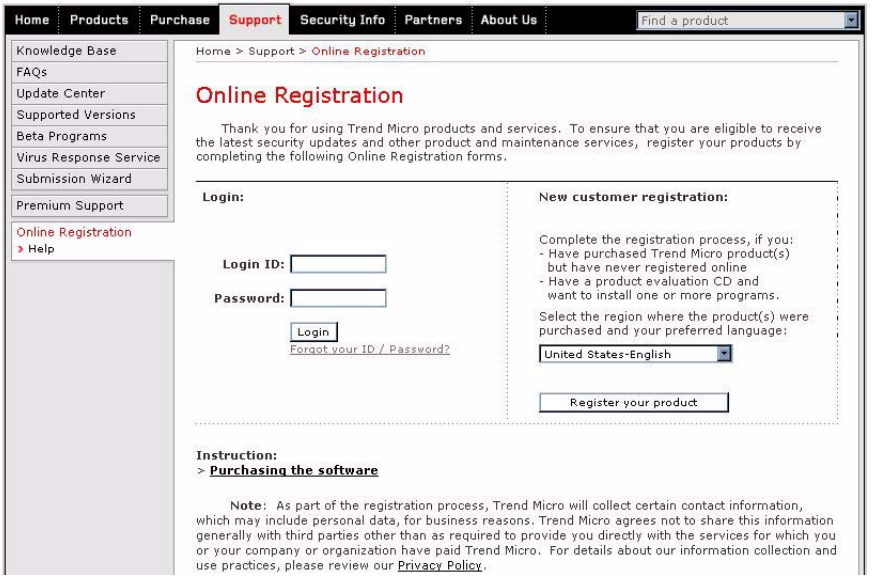


FIGURE 3-17. Trend Micro Online Registration screen.

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 click **Log on**.

Removing IWSS

The IWSS uninstall scripts require superuser privileges. Log on as **root** to uninstall IWSS.

To remove IWSS:

1. Type `./isinst` in the directory where you install the IWSS files. The **IWSS 2.0 Setup Script** screen appears.
2. Type **2** and press **Enter**. Follow the on-screen prompts to remove the service.

Upgrading IWSS

You can easily upgrade your IWSS 2.0 release by performing the following steps.

To upgrade from IWSS 2.0 to IWSS 2.2:

Run `./isinst` from the IWSS 2.2 package to perform the upgrade. IWSS automatically detects the existence of IWSS 2.0 on your machine, and saves your configuration settings.

To upgrade from IWSS 1.0 to IWSS 2.2:

1. Remove all IWSS 1.0 components by running `./isinst` from the IWSS 1.0 or IWSS 2.2 package.
2. Run `./isinst` from the IWSS 2.2 package to perform the upgrade.

Chapter 4

HTTP Scanning and URL Blocking

After installing the HTTP scanning daemon, configure IWSS for HTTP scanning and blocking. Trend Micro recommends the following:

1. Update the virus, PhishTrap and spyware pattern files, and the scan engine (see *Updating the Virus Pattern File* starting on page 3-32, *Updating the PhishTrap Pattern File* starting on page 3-35, *Updating the Spyware Pattern File* starting on page 3-35, and *Updating the Scan Engine* starting on page 3-36 for details).
2. Enable HTTP scanning.
3. Configure large file handling.
4. Bypass specific MIME content-types.
5. Specify file types to scan.
6. Specify file types to block.
7. Configure compressed file scanning limits.
8. Configure Web site and URL string blocking.
9. Configure Access Quota policies.
10. Configure notifications.
11. Configure scan actions.
12. Configure the server designation (if you are using multiple IWSS servers).
13. Configure the user identification method.
14. Configure ICAP scan policies (if you are in ICAP mode).

Understanding Scan Configuration Options

There are trade-offs between performance and security while scanning HTTP traffic for malicious content. When users click a link on a Web site, they expect a quick response. This response, however, may take longer as the system performs virus scanning. The longer wait is the result of many factors. Content may consist of a single large file, such as streaming media and executables for download. Determining whether the file is safe requires downloading the entire file before it is relayed to the user. Therefore, users must wait for the entire file to completely download before receiving any of it. Content may also consist of many small files. In this case, the user's wait is the result of the cumulative time needed to scan.

One way to improve the user's experience is to skip scanning of large files or files that cannot harbor viruses. For example, you can skip all files with an extension of ".gif", or all files with a MIME type of "image/jpeg." Unfortunately, a file's extension or MIME type may not truly reflect the true file type.

IWSS offers a reliable way to skip files that do not need scanning. For MIME content-types that are not excluded in the **HTTP > Configuration > ICAP** or **Proxy Scan** configuration screen, IWSS inspects the first 4KB of a file to determine if the content is a safe type. If a file is a safe type, then IWSS does not need to do further checking. There is a slight performance penalty for checking the content-type, rather than the MIME content-type, but it is a much more secure means of separating files that can skip security checks versus those that cannot.

You can exclude files from scanning based on extension. This option was retained for compatibility with previous Trend Micro products, though Trend Micro recommends that you minimize the list of MIME content-types to skip. In general, relying on the scan engine to decide if a file needs to be scanned is safer than trying to pick out which file types you want to skip yourself. Firstly, the content-type HTTP header may not accurately represent the true type of the message body. Secondly, some types that you may think safe to skip (for example, text) may not really be safe (since scripts are text, and may possibly be malicious). One more area where you may wish to use MIME content-type skipping is where you are consciously making a trade-off in safety versus performance. For example, a lot of Web traffic is text, and the IWSS scan engine will scan all that traffic because that content may contain scripts, which can conceivably contain malicious code. But if you are confident that you are browsing an environment that cannot be exploited by Web scripts, you may choose to

add text/* to your MIME content-type skip list so IWSS does not need to scan Web pages.

Malicious code within a small file can quickly spread throughout a network. Malicious code that requires a large file for transport will propagate more slowly, because the file containing malicious code will take longer to transmit. Therefore, it is important to screen small files efficiently and completely.

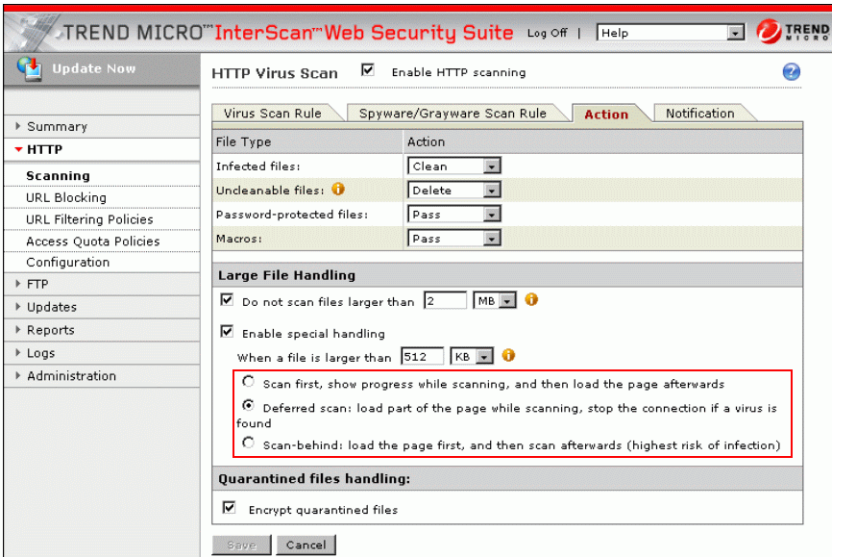


FIGURE 4-1. For large file handling, there are three options to choose from: (1) scan first, and then load page afterwards, (2) deferred scan, or (3) scan-behind.

When downloading a large file, the time to download the file and scan it for viruses may be long enough to cause the browser to time out. The size of file that you should consider “large” varies, depending on what hardware IWSS runs on, the mix of file types in the particular environment, and so on. Trend Micro recommends that files larger than 512KB (default value) be considered large; however, this value might vary depending on your network speed, server capability, and other factors.

Once you encounter a large file, IWSS handles it in one of the following ways:

- allows the file through and scans it later

- loads a part of the page while scanning
- generates a progress page to prevent the browser from timing out, thus, user does not think the connection is hung

See *Handling Large Files* starting on page 4-5 for more details.

Turning On/Off the HTTP Traffic

Open the console and click **Summary** in the left menu, and then click **Turn On** or **Turn Off** (at the top of the screen) to run or stop the HTTP traffic, respectively. **Turn Off** means that the IWSS server is shut down, thus, a client cannot connect to the outside Web server. In addition, the client cannot access the Internet unless you make adjustments in the ICAP client (for ICAP proxy) or in the browser/downstream proxy (for HTTP proxy).

Enabling HTTP Scanning

You can enable or disable HTTP scanning from the IWSS console. If you enable HTTP scanning, be sure to specify the appropriate listening port number of a given HTTP handler (default values are 1344 for ICAP and 8080 for Proxy Scan) so the traffic will go through.

For information on how to test HTTP scanning and end-user instructions on how to set the client server to point to IWSS, see *Testing URL Blocking* starting on page 3-27. For more information on the HTTP proxy topology, see *HTTP Proxy Topology* starting on page 2-7.

To enable HTTP scanning:

1. Open the IWSS console and click **HTTP > Scanning** in the left menu.
2. Select **Enable HTTP scanning**.
3. Click **Save**.

To configure the listening port number:

1. Open the IWSS console and click **HTTP > Configuration > Proxy Scan** (or **ICAP**).

2. In the **Listening port number** text box, type the port number (default values are 1344 for ICAP and 8080 for HTTP Proxy).
3. Click **Save**.

Note: IWSS handles HTTPS connections differently than the HTTP connections. Because the data is encrypted, IWSS is not capable of scanning the content. IWSS examines the initial CONNECT request, and rejects it if it does not match the set parameters (such as the target URL is on the Block List or contained in the PhishTrap pattern file, or the port number used is not defined in the `HttpsConnectACL.ini` file).

Handling Large Files

For larger files, a trade-off must be made between the user's experience and expectations, and maintaining security. The nature of virus scanning requires doubling the download time (that is, the time transferring the entire file to IWSS, scanning the file, and then transferring the entire file to the client) for large files. In some environments, the doubling of download times may not be acceptable. There are other factors such as network speed, and server capability that must be considered. If the file is not big enough to trigger large-file handling, the file will be scanned as a normal file.

IWSS offers an option called "scan-behind" to address such situations. The size of files considered "large" varies based on what hardware IWSS runs on, the mix of file types in the particular environment, and so on. In general, Trend Micro recommends that files greater than 512KB (default value) be considered large.

IWSS handles large files in one of the following ways:

- The file can be allowed through and scanned later (scan-behind)—allows the first user to download the file (whether it contains a virus or not), while IWSS scans the file after it is passed through. If a virus is found, the infected URL will be blocked for a certain period of time if the infected file is quarantined or deleted. However, if the infected file is found to be cleanable, it will not be blocked the second time it is accessed.
- A progress page is generated to prevent the browser from timing out and prevent the user from thinking that the connection is hung. IWSS downloads a complete

file to the IWSS server, then scans it, and then allows the user to get it from IWSS. If a virus is found, the appropriate warning message appears in the client's browser, and the action is applied.

- IWSS also has an option called “deferred scan”—it allows a user to get a partial file while IWSS is scanning. If no virus is found, the user gets the complete file.

For all three options, the infected URL will be blocked for a certain time. If a large file is passed immediately, and is later found to contain malicious code, IWSS takes the following actions:

- Sends a notification email message (if you enable virus notification)
- Logs the event details
- Automatically blocks the URL (for a certain period of time if the infected file is quarantined or deleted) that provided the malicious content from other users

If the affected client has up-to-date antivirus software and security patches, no further action may be needed. Otherwise, you will need to take actions to isolate and clean up the affected system. Event tracing is also necessary when you detect malicious code during an attempt to post data to the Web.

Use large file special handling if you have experienced an issue with timeouts.

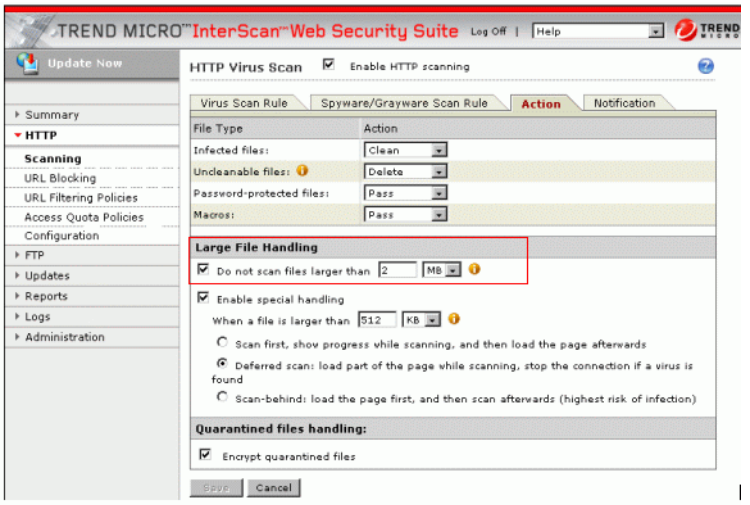


FIGURE 4-2. Under the "Do not scan files larger than" option, IWSS will not scan files larger than the size specified. This option creates a security hole. Trend Micro recommends that you only choose this option on a temporary basis; and when this option is selected, it must not be greater than 2GB.

TABLE 4-1. Comparison between scan-behind and deferred scan.

Scanning method for large file	INI setting in intscan.ini [http]	Behavior for 1st time access	URL in infectedB.ini if virus is found after scanning	Behavior for 2nd time access and thereafter to the same URL
Scan-behind	special_handling=yes deferred_scan=yes	The user always gets the file before virus scanning starts.	IWSS saves the infected URL to the [allow] section if the file is cleaned after scanning. If it is deleted or quarantined, the infected URL is added to the [block] section of the infectedB.ini file.	IWSS invokes progress page or in-line scan if a large file is cleanable. IWSS blocked the infected URL if uncleanable and quarantined or deleted
Deferred scan	special_handling=yes deferred_scan=late	The user gets the file if there is no virus. If a virus is found, IWSS drops the connection.	IWSS saves the infected URL to the [allow] section if the file is cleaned after scanning. If it is deleted or quarantined, the infected URL is added to the [block] section of the infectedB.ini file.	IWSS invokes progress page or in-line scan if a large file is cleanable. IWSS blocked the infected URL if uncleanable and quarantined or deleted

To use the large file handling for IWSS HTTP data:

1. Open the IWSS console and click **HTTP > Scanning > Action**.
2. Under the **Large File Handling** section, select **Enable special handling**, and then type the file size (in KB or MB) to be considered a large file. The default value is 512KB.
3. Select the type of large file-handling to use:
   - Scan first: show progress while scanning, and then load the page afterwards
   - Deferred scan: load part of the page while scanning, stop the connection if a virus is found (default setting)
   - Scan-behind: load the page first, and then scan afterwards (highest risk of infection)

   Note: These three options are not available for Blue Coat Port 80 Security Appliance.

4. Click **Save**.

Important Notes on Handling Large Files

- Large file special handling only applies to HTTP scanning and FTP over HTTP for stand-alone traffic, not FTP over HTTP for ICAP traffic. Users may experience timeout issues while downloading large files using FTP over HTTP.

- Using scan-behind, IWSS does not delete files subsequently found to be infected in the first affected client.

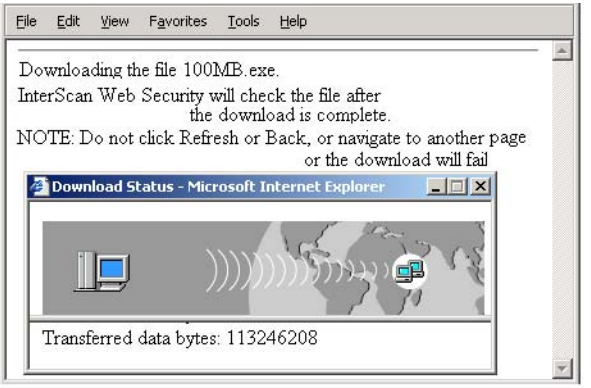


FIGURE 4-3. IWSS HTTP uses a progress window to prevent browser timeouts when downloading and scanning large files.

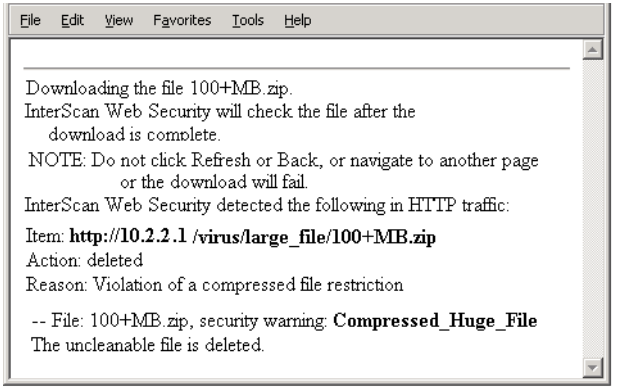


FIGURE 4-4. The user gets this notification after completing the scanning and download process.

Bypassing Specific MIME Content-types

You can configure IWSS to selectively bypass certain MIME content-types. This is not a practice that Trend Micro recommends when you enable large file handling, because it is possible for a MIME type to be forged. If you are unable or choose not to enable large file handling, IWSS must act upon the entire file. However, some file types, such as RealAudio or other streaming content, begin playing as soon as the first part of the file reaches the client machine and will not work properly with the resulting delay. You can have IWSS omit these file types from scanning by adding the appropriate MIME types to the list of MIME content-types to skip.

Note: Trend Micro recommends minimizing the list of MIME content-types to skip to reduce the risk of virus infection.

To bypass specific MIME content-types:

1. Open the IWSS console and click **HTTP > Configuration > Proxy Scan**.
2. Type the MIME content-type to bypass in the **MIME content-type to skip** field (for example, image, audio, application/x-director, video, application/pdf, and multipart).
3. Click **Save.**

To bypass specific MIME content-types (ICAP):

1. Open the IWSS console and click **HTTP > Configuration > ICAP**.
2. Type the MIME content-type to bypass in the **MIME content-type to skip** field (for example, image, audio, application/x-director, video, application/pdf, and multipart).
3. Click **Save.**

To enable anonymous FTP logon using FTP over HTTP:

1. Open the IWSS console and click **HTTP > Configuration > Proxy Scan**.

2. Type the email address for anonymous FTP logon in the field provided. ..

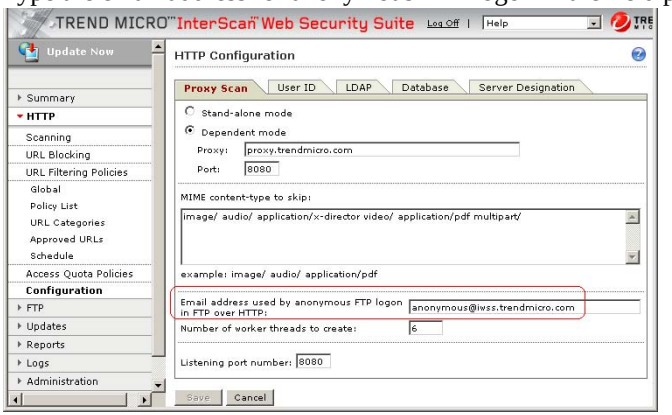


FIGURE 4-5. For HTTP proxy, use the email address as password for anonymous FTP logon in FTP over HTTP.

3. Click **Save**.

Note: FTP servers require a user ID and password for access. However, users may also anonymously log on to an FTP server. In FTP over HTTP, the proxy server acts as an HTTP proxy on the client side, but acts as an FTP client on the server side. If a client intends to log on anonymously, you need to have this email address. The configuration decides what email address is used as the password in anonymous logon.

Specifying File Types to Scan

IWSS can scan all file types, true file types (IntelliScan), or specified file types for viruses, including the individual files contained in a compressed file.

To select which file types to scan:

1. Open the IWSS console and click **HTTP > Scanning > Virus Scan Rule**.
   - To scan all file types, regardless of file name extension, select **All file types** under **Scan these file types (if not blocked)**. IWSS opens compressed files and scans all files within. Scan all files is the most secure configuration (recommended setting).
   - To use true file type identification, click **IntelliScan** under **Scan these file types (if not blocked)**.
   - You can skip files based on their extensions to work around performance issues with scanning all HTTP traffic. However, this is an unsafe practice and not recommended, because the extension of the file is not a reliable means of determining its content. You should skip files by extension only if it is necessary to meet the performance requirements of your environment.

     To scan only selected file types (Trend Micro does not recommend this setting), click **Specified file extensions** under **Scan these file types (if not blocked)**. This contains the list of all known file types that can harbor viruses. IWSS scans only those file types that are explicitly specified in the **Default Extensions** list and **Additional Extensions** text box.

     Use this option, for example, to decrease the aggregate number of files IWSS checks, to decrease overall scan time.

     Note: Do not precede an extension with a wildcard (*) character, and separate multiple entries with a semicolon.

2. Click **Save**.

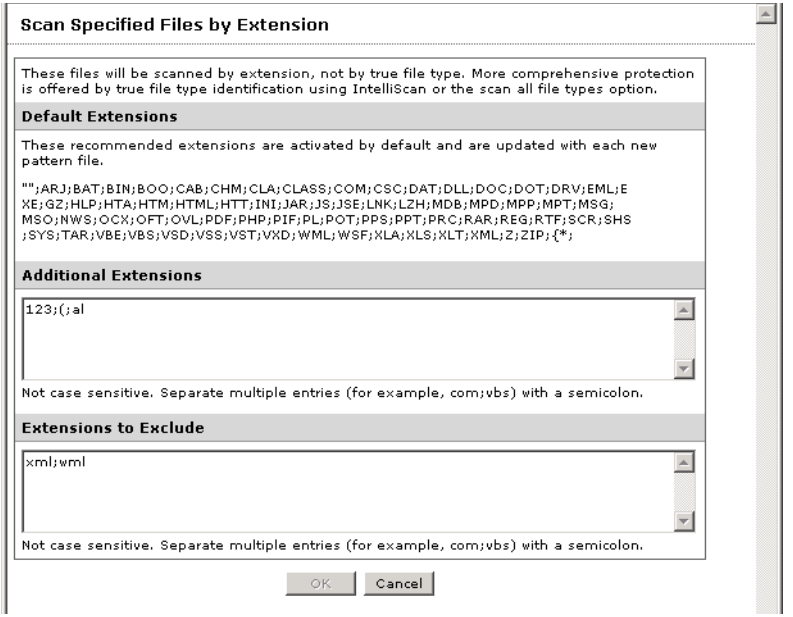


FIGURE 4-6. The recommended extensions are activated by default and are updated with each new pattern file.

About IntelliScan

Most antivirus solutions today offer you two options in determining which files to scan for potential threats. Either all files are scanned (the safest approach), or only those files with certain file name extensions (considered the most vulnerable to infection) are scanned. But recent developments involving files being "disguised" through having their extensions changed has made this latter option less effective. IntelliScan is a Trend Micro technology that identifies a file's "true file type," regardless of the file name extension.

Note: IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible to virus infection.

True File Type

When set to scan *true* file type, the scan engine examines the file header rather than the file name to ascertain the actual file type. For example, if the scan engine is set to scan all executable files and it encounters a file named "family.gif," it does not assume the file is a graphic file and skip scanning. Instead, the scan engine opens the file header and examines the internally registered data type to determine whether the file is indeed a graphic file, or, for example, an executable that has been deceptively named to avoid detection.

True file type scanning works in conjunction with Trend Micro IntelliScan, to scan only those file types known to be of potential danger. These technologies can mean a reduction in the overall number of files that the scan engine must examine (perhaps as much as a two-thirds reduction), but it comes at the cost of potentially higher risk.

For example, .gif and .jpg files make up a large volume of all Web traffic, but they cannot harbor viruses, launch executable code, or carry out any known or theoretical exploits. So, does this mean they are safe? Not entirely. It is possible for a malicious hacker to give a harmful file a "safe" file name to smuggle it past the scan engine and onto the network. The file could not be run until it was renamed, but IntelliScan would not stop the code from entering the network.

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

Specifying File Types to Block

You can identify the types of files that you want to block for security, monitoring or performance purposes. You have the option of blocking file types such as Java applets, Office documents, Audio/video files, Executables, and Images.

To specify which file types to block:

1. Open the IWSS console and click **HTTP > Scanning > Virus Scan Rule**.
2. Under **Block these file types**, select the file types that you want to block.
3. In the **Other file types** field, type the other file types that you want to block (use a space to delimit multiple entries). See *Mapping File Types to Block with MIME Content-types* starting on page B-1 for the list of other file types to block.

4. Click **Save**.

Priority for HTTP Scan Configuration

IWSS scans according to the following priority:

1. MIME content-types to skip
2. File types to block
3. File types to scan

Configuring Compressed File Scanning Limits

IWSS opens and examines the contents of compressed files according to the criteria specified in the configuration screen (**HTTP > Scanning > Virus Scan Rule**). IWSS decompresses the files for scanning according to the configurable limits (number of files, decompressed file size, decompression ratio, and decompression layers).

To configure the compressed file scanning limits:

1. Open the IWSS console and click **HTTP > Scanning > Virus Scan Rule**.
2. Under **Compressed file handling**, select from the following two options:
   - **Block all compressed files**
   - **Scan compressed files within the limits**
     If you enable **Scan compressed files within the limits**, type a value for the following parameters:
     - Number of files (default is 10000)
     - Decompressed file sizes (default is 200MB)
     - Decompression percent (1-100) (default is 100)
     - Decompression layers (0-20) (default is 10)
3. Click **Save**.

Note: "100" percent file decompression ratio means that there is no limit on the compressed files setting; whereas, "0" percent file decompression ratio means that all compressed files will be blocked.

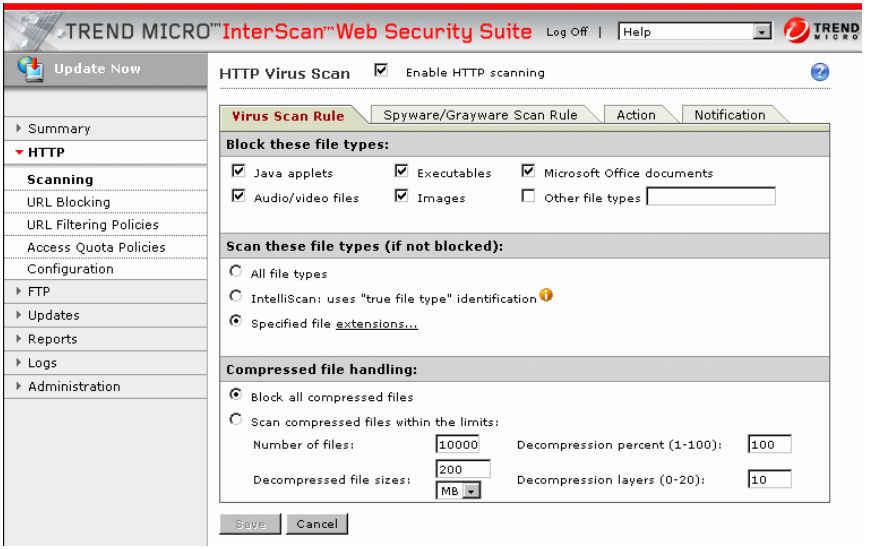


FIGURE 4-7. "Decompression percent" can be used to prevent a denial-of-service (DoS) attack against the IWSS server.

Setting the Scan Action for Viruses

See *To set the scan actions:* on page 4-20 for the procedure of setting actions when viruses are detected. You can specify the action for IWSS to take when an infected file is found (the recommended action setting is **Clean**):

- Choose **Quarantine** to move an infected file to the quarantine directory (by default, `/etc/iscan/quarantine`). The requesting client will not receive the file.
- Choose **Delete** to delete an infected file at the server. The requesting client will not receive the file.

- Choose **Clean** to have IWSS automatically clean and process infected files. The requesting client will receive the cleaned file if it is cleanable.

You can also specify the action for IWSS to take upon finding an uncleanable file, which includes worms and Trojans (the recommended action setting is **Delete**):

- Choose **Pass** to send a non-cleanable file to the client that requested it (Trend Micro does not recommend this choice, because it may allow infected files into your network).
- Choose **Quarantine** to move a uncleanable file to the quarantine directory (by default, `/etc/iscan/quarantine`). The requesting client will not receive the file.
- Choose **Delete** to delete a uncleanable file at the server. The requesting client will not receive the file.

You can specify the action for IWSS to take upon finding a password-protected compressed file (the recommended action setting is **Pass**):

- Choose **Pass** to send a password-protected file to the requesting client
- Choose **Quarantine** to move a password-protected file to the quarantine directory (by default, `/etc/iscan/quarantine`). The requesting client will not receive the file.
- Choose **Delete** to delete a password-protected file at the server. The requesting client will not receive the file.

Macro Scan

Macro Scan detects macro-containing files in file downloads and provides scanning options: Quarantine, Clean, and Pass (the recommended action setting is **Pass**).

- Choose **Quarantine** to move a macro-containing file to the quarantine directory.
- Choose **Clean** to remove macros before delivering the file.
- Choose **Pass** to disable special handling on files containing macro(s).

To set the scan actions:

1. Open the IWSS console and click **HTTP > Scanning > Action**.
2. Select the appropriate action for the following files:
   - Infected files (Delete, Quarantine, Clean)
   - Uncleanable files (Delete, Quarantine, Pass)
   - Password-protected files (Delete, Quarantine, Pass)
   - Macros (Quarantine, Clean, Pass)
3. Click **Save**.

Note: If you enable **Encrypt quarantined files** under **Quarantined files handling** (**HTTP > Scanning > Action**), the scan engine encrypts those infected files before copying them. This is to protect against accidentally executing those files. If you disable the setting, the scan engine copies the infected files to the quarantine directory in their original form.

Setting Virus Notifications

When IWSS detects malicious code in a file, which a user requested, IWSS can automatically send a customized email message. IWSS uses the Web browser of the requesting client to notify the user whenever a downloaded file is infected or blocked due to security settings.

Configure user notification messages under **HTTP > Scanning > Notification**. By default, the warning message displays information about the threat, including the threat name, file name, and action taken.

To configure the Administrator Notification settings:

1. Open the IWSS console and click **HTTP > Scanning > Notification**.
2. Under **Administrator Notification**, select the trigger events for sending a notification:
   - Virus
   - Trojan
   - Other malicious code

   To receive a notification when a file is blocked, enable **Send a message when a file is blocked**.

   If you do not want to use the default notification messages, highlight the default text and type your own version. If applicable, insert variables in the text as described in *Using Variables in Notifications* starting on page 4-22.
3. Configure the email settings by clicking  on the **Notification** screen. Type a value for each configuration field:
   - Email address of the receiver of the notification messages in the **To address(es)** field. Use a comma as delimiter for multiple email addresses
   - Email address of the sender of the notification messages in the **Sender's email address(es)** field
   - Domain name or the IP address of the mail server that will send the notification messages in the **Server name or IP address** field (the default is localhost)
   - Port used by the mail server, typically 25, in **SMTP server port**
   - Frequency that the mail queue must be checked in the **Check mail queue in minutes** field
4. Click **Save**.

To configure the User Notification Messages settings:

1. Open the IWSS console and click **HTTP > Scanning > Notification**.
2. Under **Headline**, type the header line that will be displayed in the browser. The header line is common for virus infection messages, file type blocking, and URL blocking messages.
3. You can provide additional information to the users (virus warning messages for upload and download, warning messages for file type and URL blocking).

   To configure a notification message:

a. Click **Default** to display only the default warning message.

b. Click **Customized**. Type the additional message in the **Customized Message** text box, or

c. Click **Both** to display the default message followed by the customized message.

d. Click **Save**.

4. Click **Save**.

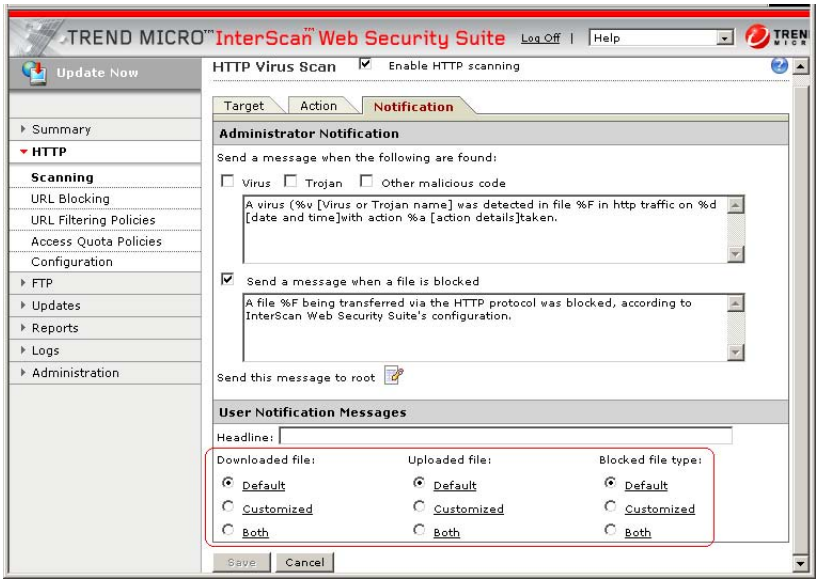


FIGURE 4-8. "Both" appends your message to the default message.

Using Variables in Notifications

Notifications are a management tool that inform you a security event has occurred, despite the protection provided by your IWSS software. To make notifications more meaningful, IWSS uses variables as placeholders in a notification. When an event occurs, IWSS substitutes the specific information in place of the variable, giving you more information about the event.

For example, you could create a generic notification as follows: “A virus was detected in HTTP traffic.” This notification lets you know there is a problem, but does not provide much information to help you follow up.

Instead, you could set up the notification using variables as follows: “%v was detected in %F in the HTTP traffic on %d.” The notification might read as follows:

“WORM_SASSER.B was detected in mywork.htm in the HTTP traffic on 12/18/2004 11:59:52”

With this information, you can now zero in more quickly to clean up the problem before it spreads. The notification in this example uses three variables: %v, %F , and %d.

TABLE 4-2. Description of variables

Variable	Variable Meaning	How the Variable is Used
%a	action details	The action taken on the infected file, for example, Quarantine
%d	date and time	The date and time of the triggering event
%F	file name	The name of the file in which a threat is detected, for example, anti_virus_test_file.htm
%s	server name	The name of the affected server
%v	virus or Trojan name	The name of the threat detected

URL Blocking

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

Note: Configure the ICAP client to scan files in pre-cache request mode to make this feature work. The stand-alone proxy requires no additional configuration.

You can explicitly specify the Web sites and URL strings to block (or to exempt from blocking).

Using this feature, you can block a given site yet allow access to some of its sub-sites. You can also import a list of Web sites and URL strings from a given file.

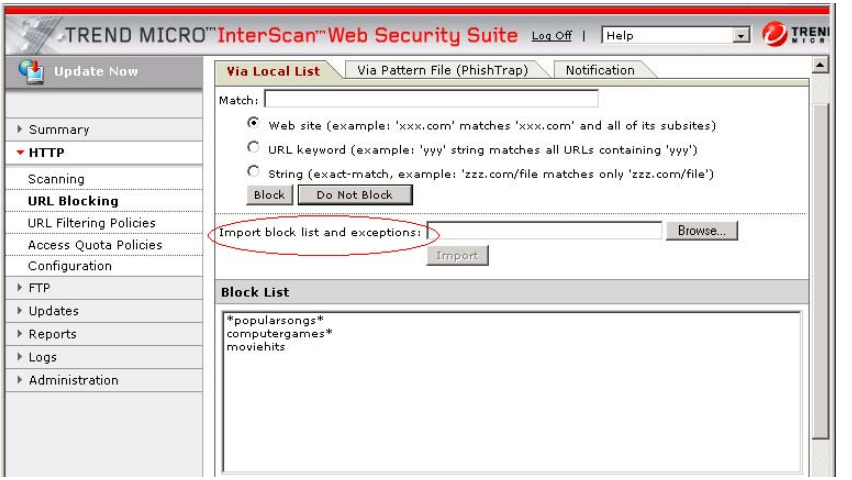


FIGURE 4-9. To import a file that contains a list of Web sites, URL keywords, or strings, make sure that you write "URL Blocking Import File" on the first line of that file. Use [block] and [allow] headings for the block and exception list, respectively.

To enable URL blocking:

1. Open the IWSS console and click **HTTP > URL Blocking**.
2. Select **Enable URL blocking**.
3. Under **HTTP > URL Blocking > Via Local List**, type the full Web address or URL keyword, or exact-match string in the **Match** field. Identify this entry by selecting one of the three options:
   - Web site
   - URL keyword
   - String
4. Click **Block** to include this entry in **Block List**. Click **Do Not Block** to include this entry in **Exceptions to the Block List**.
5. Click **Remove** to remove the highlighted entries from the list (or **Remove All** to remove all entries).
6. To import a list of Web sites and URL strings from a given file to **Block List** and **Exceptions to the Block List**, specify the location of the file in the **Import block list and exceptions** field by clicking **Browse**, and then click **Import**.

   To identify a folder or directory in a given Web site, use a forward slash (/) after the last character. For example, if you want to block `www.blockedsite.com` but allow access to its `charity` directory:

   a. Type `www.blockedsite.com` in the **Match** field, and then click **Block**.

   b. Type `www.blockedsite.com/charity/` in the **Match** field, and then click **Do Not Block**. (If you write `charity` without the forward slash, IWSS will consider `www.blockedsite.com/charity` as a file.)

   c. Click **Save**.

   Write `URL Blocking Import File` on the first line of a file that contains a list of Web sites, URL keywords, or strings, and then write one rule per line. Group them under `[block]` or `[allow]` section. For example:

```
URL Blocking Import File
[block]
*virus*
virus
*sasser*
[allow]
```

```
www.trendmicro.com*
www.antivirus.com*
```

7. Click **Save**.

Note: To include the "*" and "?" characters in a URL blocking string rather than having IWSS consider them as wildcards, use variable %2a or %2A to represent ***** and variable %3f or %3F to represent **?**. For example, to block `www.example.com/*wildcard` literally, specify the blocking rule as `www.example.com/%2awildcard` instead of `www.example.com/*wildcard`.

FIGURE 4-10. You can use case-sensitive variables in the "Customized Message" field.

PhishTrap Overview

Phishing is a malicious hacker term that means hunting for a victim. "Phishers" imitate an email message from a company with whom the user has an account. These fraudulent email messages seem authentic, and many recipients are deceived into supplying their personal information.

PhishTrap is a Trend Micro service that leverages:

- the ability of IWSS to block outbound access to a specific URL

- the capability of the Trend Micro antivirus team to collect and analyze customer submissions and distribute a database of known harmful URLs

PhishTrap can stop the harm coming from information that is sent out from the client, such as private data/information. PhishTrap prevents access to known phishing URLs. Thus, blocking the URL is appropriate in this case.

The URL that is determined to maliciously collect user information will be added to the PhishTrap pattern file. The PhishTrap pattern file is a list of URLs that IWSS will block. IWSS will periodically retrieve the updated PhishTrap pattern file via ActiveUpdate.

IWSS allows users to submit suspected phishing URLs to TrendLabs for evaluation. TrendLabs will evaluate the Web site to determine whether the submitted URL is malicious. The URL is considered malicious if it meets the criteria for one of the categories listed below.

- **Phishing**: a fraudulent collection of confidential information. This can be done by offering an email message or Web site that poses as a communication from a legitimate business, which requests personal information to commit fraud or other crimes
- **Spyware**: A hidden but legal program that secretly collects confidential information. Spyware monitors a user's computing habits and personal information, and then sends this information to third parties without the user's approval.
- **Virus accomplice**: An outbound HTTP request due to known behavior of malicious code — the malicious code could either send the information out or download further components from a certain URL
- **Disease vector**: A Web site that exists only for a malicious purpose

To block different PhishTrap categories:

1. Open the IWSS console and click **HTTP > URL Blocking > Via Pattern File (PhishTrap)**.
2. Enable the following PhishTrap categories that you want to block:
   - Phishing: fraudulent collection of confidential information
   - Spyware: hidden but legal program that secretly collects confidential information

- Virus accomplice: outbound HTTP accesses due to known behavior of malicious code
- Disease vector: a Web site that exists for a malicious purpose

3. Click **Save**.

To submit a suspected phishing URL to TrendLabs:

1. Open the IWSS console and click **HTTP > URL Blocking > Via Pattern File (PhishTrap)**.
2. Type the suspected site in the **PhishTrap URL** field.
3. Select the categories (Phishing, spyware, virus accomplice, disease vector, and others) from the drop-down menu under **PhishTrap categories**.
4. Type the sender's email address.
5. Click **Submit**.

To enable spyware scanning:

1. Open the IWSS console and click **HTTP > Scanning > Spyware/Grayware Scan Rule**.
2. Select spyware and other grayware categories for scanning.
3. Click **Save**.

Note: When spyware scanning is enabled, IWSS detects spyware and takes the same action as specified for the uncleanable virus setting.

User Notification Messages

When IWSS detects an attempt to access a URL in the PhishTrap pattern file, a warning screen appears in the browser of the requesting client. The message states that the suspected URL has been blocked because it is in the PhishTrap pattern file.

To configure a user notification message:

1. Open the IWSS console and click **HTTP > URL Blocking > Notification**.
2. Under **User Notification Messages**, choose one of the three options:
   - Click **Default** to display only the default warning message.

- Click **Customized** to display your own version of warning message — type the additional message in the **Customized Message** text box
- Click **Both** to display the default message followed by the customized message.

3. Click **Save**.

FIGURE 4-11. A sample URL blocking message for the disease vector group.

Access Quota Policies

You can enforce access quotas based on the HTTP bandwidth used per unit of time. IWSS gives you the option to set a quota for IP address/range, host name, and user/group name in a given quota interval (daily, weekly, monthly) for the whole system. IWSS saves the access quota policies in a database (see *Setting up the Database* starting on page 4-31 for more details). After making any changes (adding or deleting) to the quota policy, the IWSS service in a multiple server configuration environment reloads the policies accordingly within the time-to-live (TTL) value.

If the quota is exceeded while making a download, the download will be allowed to continue. However, the succeeding downloads/browsing (before the access quota interval expires) will fail. Users are allowed access again after the access quota interval expires. For a group quota policy, the quota is for each member instead of the whole group, and this is the same for a given range of IP addresses.

To configure the access quota policies:

1. Open the IWSS console and click **HTTP > Access Quota Policies**.
2. Select **Enable access quota control**.
3. From the drop-down menu select the access quota interval (Daily, Weekly, Monthly).
4. Click **Save**.
5. Click **Add Policy** to create a new policy.
6. In the **Access Quota Policy: Add Policy** screen, select **Enable policy** and click one of the following two options:
   - (Daily, Weekly, or Monthly) access quota in MB (type the size in MB): Set the Web browsing and HTTP file download quota. Users who reach their quota will be able to finish their current download, but will receive a notification in their Web browser upon their next Web access attempt. The quota is automatically reset at the end of the specified time period.
   - Unlimited access: Choose this option to exempt the user(s) or groups you define in Accounts from any quota limits. If a user is a member of more than one policy, the policy with the highest priority is given precedence.

7. Under **Accounts**, identify the type of accounts (IP address/range, host name, user/group name).

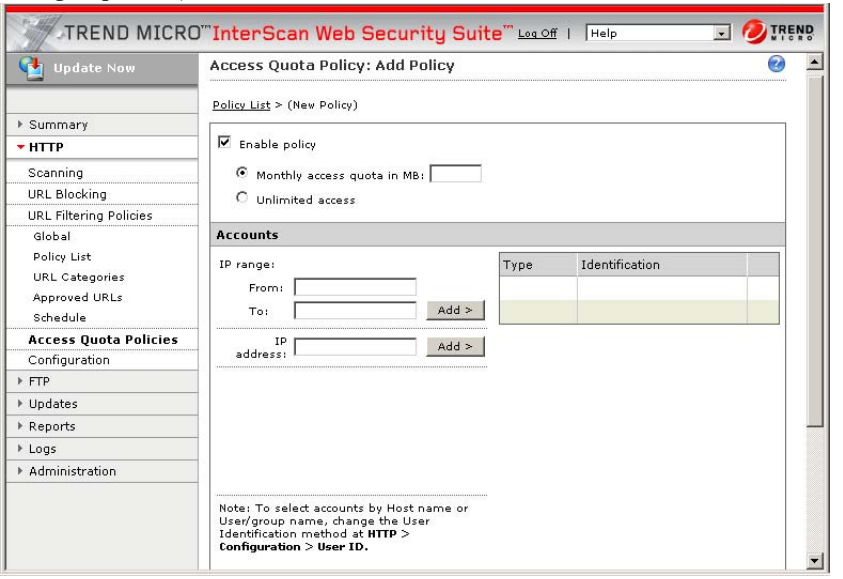


FIGURE 4-12. The options shown in the Accounts section depend on the user identification method configuration (HTTP > Configuration > User ID).

8. Click **Save**.

Note: TTL indicates the number of minutes to implement the changes of a new policy. To deploy the changes on the account(s) immediately, click **Deploy Policies**.

Setting up the Database

Make sure that you set up your database appropriately under the **Database Connection Settings** section (**HTTP > Configuration > Database**). When you are setting up a database for multiple IWSS server configurations, you need to designate the same database server for all IWSS servers (see *Configuring Server Designation* starting on page 4-34 for more details). The IWSS package installs the PostgreSQL

7.4.1 database. IWSS also supports Oracle 8i/9i. For both types of database, the schema (that is, table definitions, stored procedures, and so on) used by IWSS is initialized during installation.

To configure the database connection settings:

1. Open the IWSS console and click **HTTP > Configuration > Database**.
2. Under **Database Connection Settings**, type a value for the following parameters:
   - ODBC data source name
   - Logon name
   - Password
3. Click **Save**.

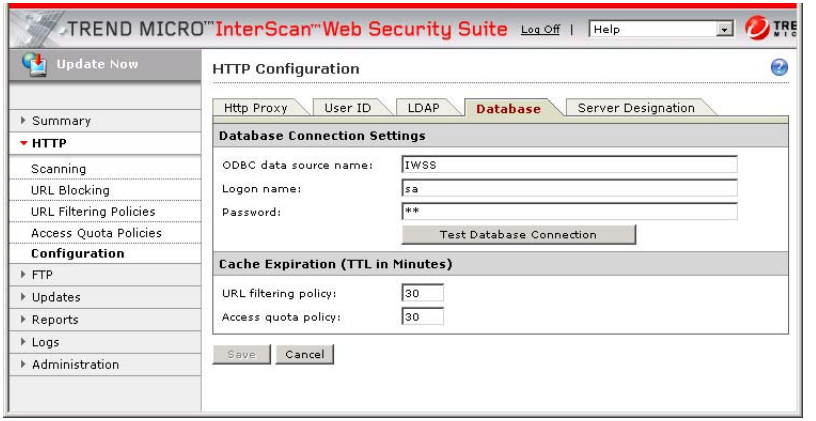


FIGURE 4-13. To verify that the database connection is working, click "Test Database Connection."

To configure Time to Live (TTL):

1. Open the IWSS console and click **HTTP > Configuration > Database**.
2. Under **Cache Expiration (TTL in Minutes)**, type a value for the following parameters:
   - URL filtering policy
   - Access quota policy

3. Click **Save**.

To configure the LDAP settings:

The purpose of LDAP configuration is to link the user and group information with the Active Directory. Through this setup, you can authenticate based on the Active Directory list. You need to obtain the LDAP connection information from your Active Directory administrator. See *User Identification Process* starting on page 2-18 for the details on user/group name via proxy authorization (using LDAP for account information).

1. Open the IWSS console and click **HTTP > Configuration > LDAP**.
2. Under **LDAP Settings**, type a value for the following parameters:
   - LDAP server hostname: Type the host name of the LDAP server you will use
   - Listening port number: Type the port number the LDAP server will use to receive requests from the IWSS server
   - LDAP admin account: Type administrator-level log on credentials for the LDAP server
   - Password: Enter the password for the account above
   - Base distinguished name (served as a starting point for LDAP search operation): Enter the LDAP distinguished names for country, network, and organization separated by a comma
   - Authentication method (select **Simple** to pass the admin password as plain-text or **Advanced** to use the Kerberos authentication)
3. Under **Kerberos Authentication Settings**, type a value of the following parameters:
   - Default realm—the default Kerberos principal realm that the user belongs to. A Kerberos realm refers to the set of Kerberos principals registered within a Kerberos server (Kerberos realm are case sensitive and normally are all in upper case)
   - Default domain—the Internet domain name that maps to the default Kerberos realm
   - KDC and admin server—the KDC and the admin server for the default realm. KDC is the machine and software that perform the role of a trusted arbitrator in the Kerberos protocol

- KDC port number—the Key Distribution Center (KDC) server listening port number

4. Click **Save**.

Note: To check if the LDAP connection is working, click **Test LDAP Connection**.

Configuring Server Designation

Using multiple servers, IWSS is scalable to any configuration you need. This works because HTTP requests on one server can be processed independently of HTTP requests on other servers.

You can deploy HTTP in a multiple server configuration (in this case, you need to set up a database in a central location, see *Setting up the Database* starting on page 4-31 for more details) in two ways:

- Multiple IWSS ICAP servers that work with a single ICAP client for load balancing
- Multiple HTTP stand-alone servers that use a Layer 4 switch for load balancing

One IWSS server must be designated as "master," and the configuration files must be synchronized manually, via Control Manager or via a customer-created script. You need a Layer 4 switch to load balance between IWSS servers for multiple HTTP stand-alone servers. However, for multiple ICAP servers, you need an ICAP client with load balancing capability. To access the administrator console for each IWSS server, you need to configure the private IP addresses.

Note: For a multiple server configuration setup, Trend Micro recommends using a Layer 4 switch or other appliances that can perform the load-balancing function.

IWSS gives you the option to synchronize dynamic information across IWSS servers in a farm. There are two kinds of IWSS data that require synchronization between servers:

- URLs that are blocked because a virus is detected: this data is available to all servers for URL blocking to be most effective. Any real-time data synchronization mechanism must be shared between data types. Thus, one server

must be designated as a master for such data (see *To configure server designation:* starting on page 4-35 for details)

- Amount of data received by a given user, which is used to enforce an access quota: a central database must be set up for this purpose (see *To configure the database connection settings:* starting on page 4-32 for details)

To configure server designation:

1. Open the IWSS console and click **HTTP > Configuration > Server Designation**.
2. Select **Enable for use in a multiple IWSS server configuration**.
3. Type a value for the listening port number of the master server.
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. When updating the settings, remember to also update the settings of the other IWSS servers in your network.*

5. Click **Save**.

FIGURE 4-14. Entries in the URL block list in memory are dynamically added to all IWSS servers in a farm.

Configuring User Identification Method

IWSS helps to trace security events to the affected systems. IWSS includes three event-tracing identification methods:

- IP address (default setting)
- Host name (modified HTTP headers)
- User/group name via proxy authorization (use LDAP for account information)

See *User Identification Process* starting on page 2-18 for more detailed information.

Note: If you select the "User/group name via proxy authorization" option, make sure that LDAP is successfully configured (see *To configure the LDAP settings:* starting on page 4-33 for more details), or the IWSS server will not start.

To configure the user identification method:

1. Open the IWSS console and click **HTTP > Configuration > User ID**.
2. Select one of the following four options:
   - IP address
   - Host name (modified HTTP headers)

   Note: To be able to use the Host name option, all clients must run the `register_user_agent_header.exe` tool, which can be found in `opt/trend/IWSS/ISHTTP/IScan.HTTP/`.

   - User/group name via proxy authorization (use LDAP for account information)
   - No identification

3. Click **Save**.

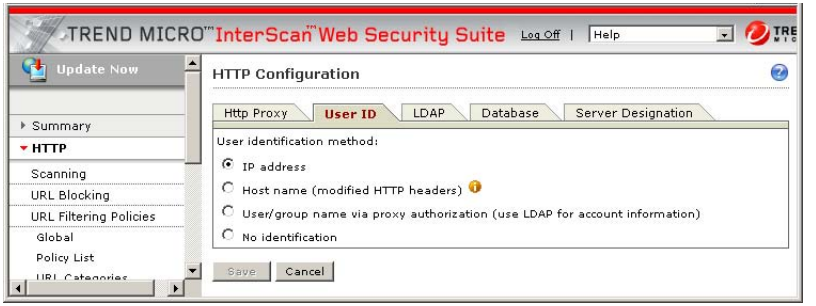


FIGURE 4-15. "IP address" is the default user ID method setting.

ICAP and Proxy Scan Policies (Process)

You can fine-tune the performance of IWSS by adjusting the number of processes spawned upon startup and the refresh rate of idle processes. In addition, you can limit the total number of child processes IWSS will use at any one time, and the total number of child processes spawned for a given thread. Configure the settings on the IWSS console and click **HTTP > Configuration > ICAP** or **Proxy Scan**.

Note: Improperly adjusting the settings can result in system instability. We recommend that you use the defaults unless there is a specific performance-based reason to alter them.

Pre-spawning processes

When you start IWSS, by default it will create 15 child processes to handle the traffic load. Depending on your system resources and traffic load levels, you may want to increase the value in the **Number of pre-spawned processes** field. There is no

maximum allowed value. However, entering too high a value results in wasted system resources.

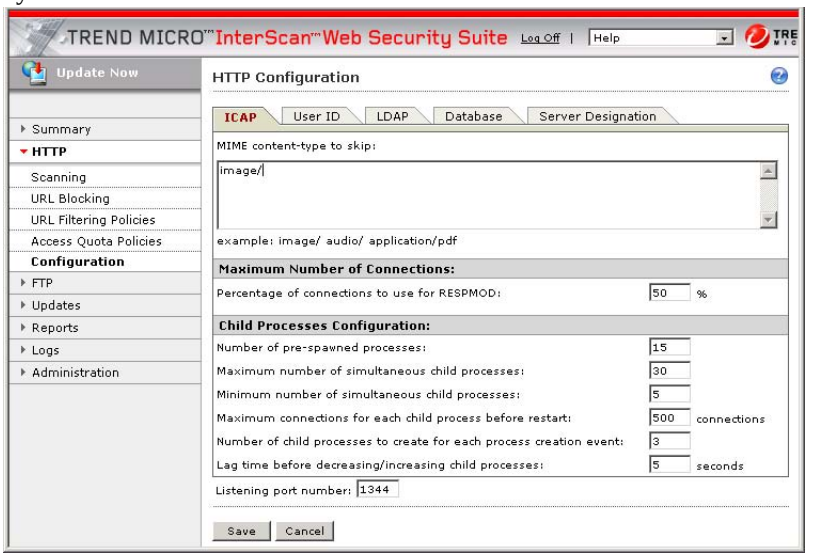


FIGURE 4-16. ICAP Process mode.

Limiting child processes

IWSS uses a number of child processes to handle scanning, analysis, and forwarding of HTTP messages. As traffic levels vary, IWSS will increase or decrease the amount of active child processes to maintain a balance between the available system resources and proxy response time. Specify the maximum number of child processes that can be created in the **Maximum number of simultaneous child processes** field, and the minimum number that will be kept running in the **Minimum number of simultaneous child processes** field.

Before creating a new child process, IWSS checks first to see if there are any existing processes that can be used. If there are none, IWSS creates a new one. Although there is typically no need to limit the number of child processes IWSS can create, this option allows you to set a maximum. This gives you the control not to exhaust all system resources. The stand-alone proxy mode works best with as many processes as the system will support. Each process consumes around 30MB of virtual memory.

Use this fact to estimate the number of processes the available virtual memory will support. ICAP requires fewer processes, because the ICAP client serves to concentrate HTTP requests into a smaller number of sessions.

Extinguishing old connections

IWSS stops child processes after a set number of connections have been handled to ensure that idle resources do not consume unnecessary memory. A typical number to enter in the **Maximum connections for each child process before restart** field is 500, meaning that after 500 HTTP connections have been handled, the hosting child process itself is terminated, and a new one generated (a new child is only created if needed). Setting this number too low can result in needlessly brief cycles. Enter a zero (0) in this field to disable the maximum number of connections. The default value is 500.

Selecting how many child process to create

You can limit the number of active connections that IWSS will spawn from a given child process before creating a new child. Type the value in the **Number of child processes to create for each process creation event** field. The default value is three.

Lag time before increasing/decreasing child processes

In Process mode, the daemon uses a pool of child processes to handle network connections, and it dynamically alters the size of this pool depending on the amount of network traffic. The parent process will periodically check its workload to determine whether it must add more child processes or stop some of the idle child processes. Roughly every second, the parent checks if fewer than 10% of its child processes are idle, and if so it marks itself as busy. Conversely, if more than 50% of its child processes are idle it marks itself as not busy.

If the parent marks itself in the same state for a consecutive number of intervals equal to the value set in the **Lag time before decreasing/increasing child processes** field, then it will either spawn more child processes (if it is busy) or stop existing idle child processes (if it is not busy). Increasing this value makes the daemon respond more slowly to swings in the level of network traffic, but decreasing it too much will cause

the daemon to waste more CPU time in the overhead of creating and destroying child processes. The default value is 5 seconds.

ICAP and Proxy Scan Policies (Thread)

The IWSS scan policies contain configurable parameters, such as the value of the maximum number of connections for request and response service, and number of threads to create. Click **HTTP > Configuration > ICAP** or **Proxy Scan** to configure the scan policies.

Maximum number of connections for REQ service

In this field, indicate the maximum number of simultaneous ICAP REQMOD (request mode) connections the IWSS server will handle, and will report to the ICAP client in response to an OPTIONS request (the default value is 150). The ICAP client will stop requesting new connections once this number of connections has been established, and will instead begin to pipeline additional ICAP requests through the existing active connections. Increasing this number may increase throughput, at least until IWSS consumes all available CPU cycles. In general, fewer REQMOD connections are necessary than RESPMOD (response mode) because each REQMOD request is processed much more quickly.

Maximum number of connections for response modification service

See the description for REQ connections above, except this value indicates the maximum number of RESPMOD connections reported by the IWSS server to the ICAP client (default value is 250).

Number of worker threads to create

This configuration parameter sets the number of worker threads for the service to launch (default value is 6). In threaded mode, each worker thread can handle many connections, so lowering this number does not directly influence the number of simultaneous connections you can service. Ideally there must be enough threads running so that if one thread is waiting for disk I/O, another can be processing

network traffic, but not so many threads that the system gets slowed down with overhead.

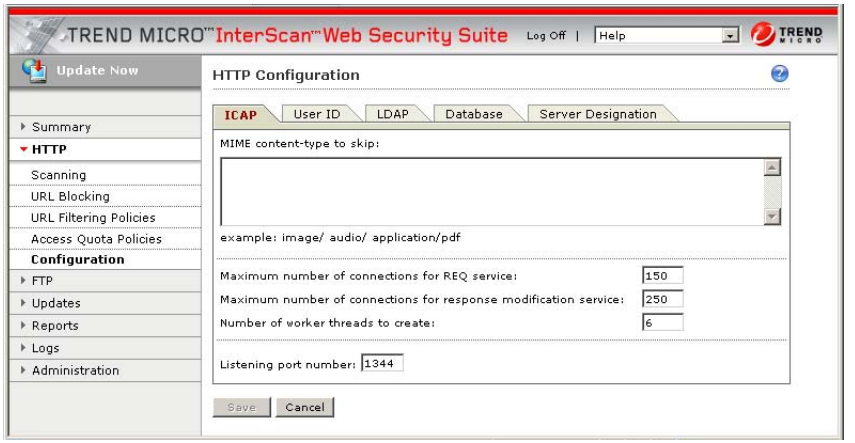


FIGURE 4-17. ICAP Thread mode.

Note: For **Number of worker threads to create**, Trend Micro recommends setting this value to three times the number of CPUs running on your IWSS machine. For installation on a dual-CPU machine, set the value to 6.

Chapter 5

URL Filtering

This chapter presents an overview and workflow of the IWSS URL filtering module with step-by-step instructions for creating and configuring policies.

Topics included in this chapter are:

- URL Filtering Overview
- URL Filtering Workflow
- Configuring URL Filtering Policies
- URL Filtering Policy Introduction
- Enabling URL Filtering
- Creating a New Policy
- Modifying an Existing Policy
- Configuring the URL Filtering Approved List
- Configuring Work Time Settings
- Requesting URL Classification Review
- Regrouping Categories

URL Filtering Overview

The default settings for the IWSS URL filtering module assume that your primary interest is to avoid legal liabilities associated with viewing of offensive material. However, because there are instances that require exceptions, additional policies may be created to allow access to restricted category groups (that is, users whose job function requires broader access). For example, members of the Human Resources department may need unrestricted Internet access to conduct investigations into violations of your organization's acceptable Internet use policies.

In addition, IWSS can enhance productivity as it combines dynamic filtering with advanced databases. Unrestricted access to the Internet can result in reduced worker productivity and decreases bandwidth available for legitimate business purposes. Some examples of Internet use that may reduce employee productivity are online trading, shopping, auction bidding, selling, searching work, dating, gambling and other non-work related activities. IWSS allows the Internet to be made available to corporate users according to user and workgroup-specific needs, thus optimizing the use of the Internet.

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

1. The assignment of a sub-category to a category group is completely configurable. The sub-categories are organized into six category groups:
   - Company Prohibited Sites
   - Not Work Related
   - Possible Research Topics
   - Business Function Related
   - Customer Defined
   - Others
2. Each category group may be blocked or not blocked.
3. The blocking rules that are associated with the category groups may be configured differently for different IP addresses, IP ranges, users/groups, and host names.

Access to all identified URLs within a targeted category may be managed according to policy. The database associates each URL with a set of categories. It is possible that a URL may be wrongly categorized, in which case, the URL Filtering Approved

List can be used to override the classification of the URL. The patterns specified in the URL Filtering Approved List are matched against the URL, not to the contents of the document that the URL refers to. You can use the URL Filtering Approved List to bypass internal Web sites and other sites where the attempt to classify them introduces unnecessary overhead.

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

- Block during work time
- Block during leisure time

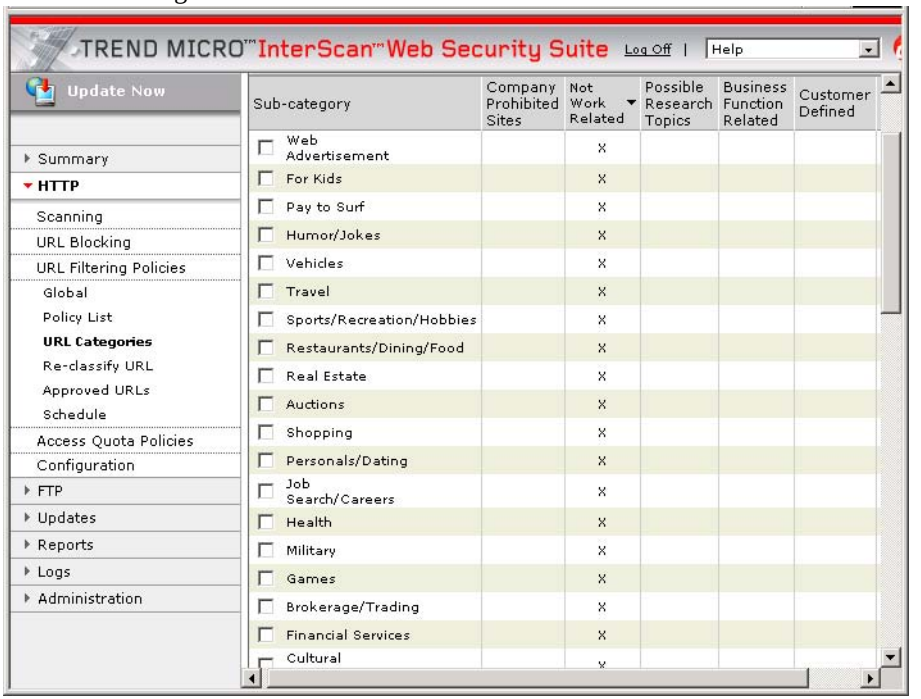


FIGURE 5-1. Sub-categories under the "Not work related" category.

URL Filtering Workflow

The input for the URL filtering module consists of the URL (Filtering Policy) and the user's ID (IP address, IP address range, user, group name, or host name). A user is identified according to the "user identification method" that IWSS is configured to use (see *User Identification Process* starting on page 2-18 for details).

Note: The network configuration may determine whether some user identification methods can be used. For example, the client IP address will not be available if IWSS is used as an upstream proxy.

The output of the URL filtering module is either:

- Allow access to the URL (pass), or
- Deny access to the URL (block)

The URL filtering module works with the local classification database and the policy management database.

- A local classification database contains the URL classification information; thus, most classifications will be retrieved with a minimum of overhead.
- If the classification information is not available locally, a remote Web-based classification service is contacted.

The classification service may have more up-to-date information, or may be able to classify the URL dynamically. The classification service compiles a list of previously unclassified URLs. Once classified, these URLs are added to a master database, which is distributed as an update to the local IWSS classification database. Such updates are periodically retrieved by IWSS via ActiveUpdate.

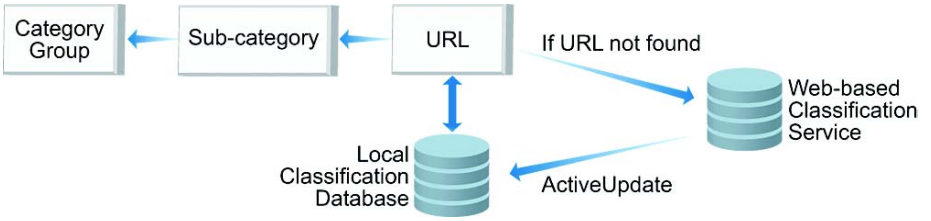


FIGURE 5-2. Working mechanism of URL classification.

A queried URL is classified into one of over fifty sub-categories, and then mapped into one of six Category Groups (Company Prohibited Sites; Not Work Related; Possible Research Topics; Business Function Related; Customer Defined; and Others). With the given Category Groups classification and the user ID as input, the query is made to the policy management database. The result of the query is either allowing or blocking access to the requested URL.

Note: Your corporate internal Web sites must not be classified; thus, such sites must be added to the URL Filtering Approved List to prevent unnecessary overhead (see *To configure the URL filtering approved list:* starting on page 5-12 for details).

Manual updates to the URL filtering database can be done under the **Summary** > **Scanning** screen of the IWSS console.

Configuring URL Filtering Policies

IWSS uses user/group based policy management for URL filtering and access quota management, which requires a mechanism for retrieving/maintaining a list of policies. The IWSS policy model allows policies to be associated with various entity types such as user, group, IP address, a range of IP addresses and host names. IWSS passes a query criteria that includes keywords for each entity type to the query interface. The policy query module then looks into the policy store and generates a result set, which contains a list of policies that fulfill the query criteria. The caller module can use this result to determine what action is needed.

The following are essential elements in configuring URL filtering policies:

- Enabling URL filtering
- Creating a new policy
- Modifying an existing policy
- Setting what category groups the policy blocks
- Setting the priority list
- Regrouping categories
- Configuring work time settings

URL Filtering Policy Introduction

The IWSS URL filtering policy consists of the following three elements:

- **Entity**
- **Policy**
- **Rule**

An **Entity** is the basic element that associates with one and only one **Policy**. An **Entity** can be a user, group, IP address, IP address range, or host name. These services tie into a directory and identify particular users. User identification ties into **Policy** to ensure that each individual receives access to the correct Web sites. A **Policy** is a set of guidelines or certain restrictions that a company wants to enforce for management purposes. This component determines individual user actions such as the users who can access specific Web site sub-categories during different time periods. Each **Policy** can contain one or many **Rules**, and each **Rule** has its own effective time period and it contains certain types of information that will be applied to the **Entity**. In the case of IWSS URL filtering, each **Policy** has two **Rules**:

- Work time
- Leisure time

Each **Rule** has its own setting for blocking or passing certain URL category groups. Create these elements to start a policy for traffic filtering.

TABLE 5-1. Major database tables used for policy management (including URL filtering and Access Quota).

Table Name	Example Columns
tb_Policy	PolicyName, PolicyType
tb_Rule	PolicyID, ActiveTime
tb_QuotaConsumption	EntityType, Consumption
tb_EntityType	EntityTypeName
tb_PolicyType	TypeName, TimeToLive
tb_Entity	EntityType, EntityName
tb_PriorityList	EntityID, PolicyID, Priority

Enabling URL Filtering

Make sure that the URL filtering function is enabled before you start. You can enable URL filtering from one of the **URL Filtering Policies** screens (**Global**, **Policy List**, **URL Categories**, or **Schedule**).

To enable URL filtering:

1. Open the IWSS console and click **HTTP > URL Filtering Policies > Global** (or **Policy List** or **URL Categories** or **Schedule**).
2. Select **Enable URL filtering**.
3. Click **Save**.

Creating a New Policy

When you are creating a new policy or modifying an existing policy, the following steps must be performed:

- Select accounts
- Specify rules

To select the account type, first configure the **User identification method** setting at **HTTP > Configuration > User ID** and click **Save**.

To create a new policy:

1. Open the IWSS console and click **HTTP > URL Filtering Policies > Policy List**.

2. Click **Add Policy**.

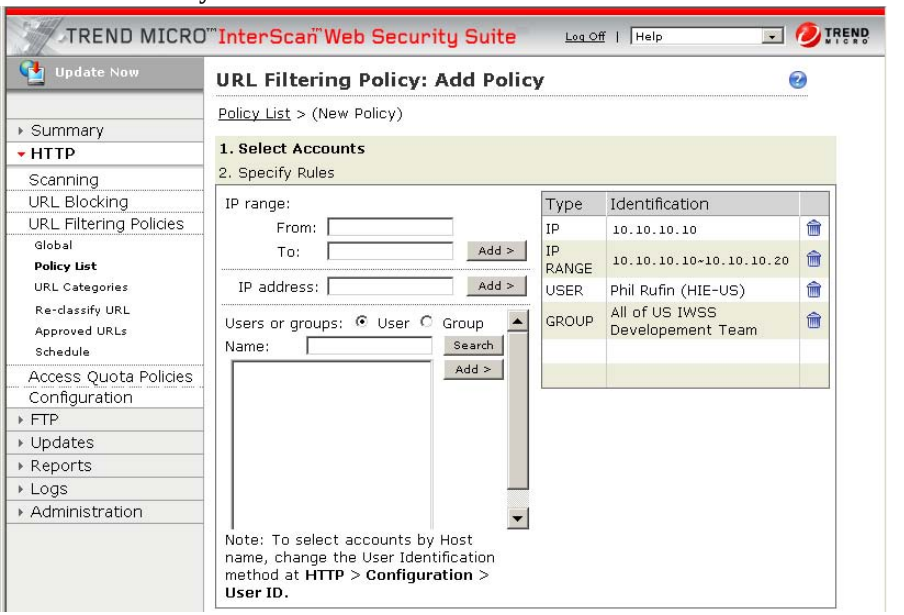


FIGURE 5-3. To select an account by host name, change the "User Identification method" setting to "Host name (modified HTTP headers)" at HTTP > Configuration > User ID.

3. The **URL Filtering Policy: Add Policy** screen appears. Specify the account type (IP, IP range, user or group, or hostname), which was defined under **HTTP > Configuration > User ID**. Click **Add**.
4. Click **Next**.
5. Under **2. Specify Rules**, make sure that **Enable policy** is selected.
6. Type the policy name in the field provided and select the URL categories to be blocked during work and leisure time:
   - Company Prohibited Sites
   - Not Work Related
   - Possible Research Topics
   - Business Function Related
   - Customer Defined

- Others

Note: If no policies for a specific user or user group are defined in **Policy List**, IWSS applies the default policy setting in the **Global** screen.

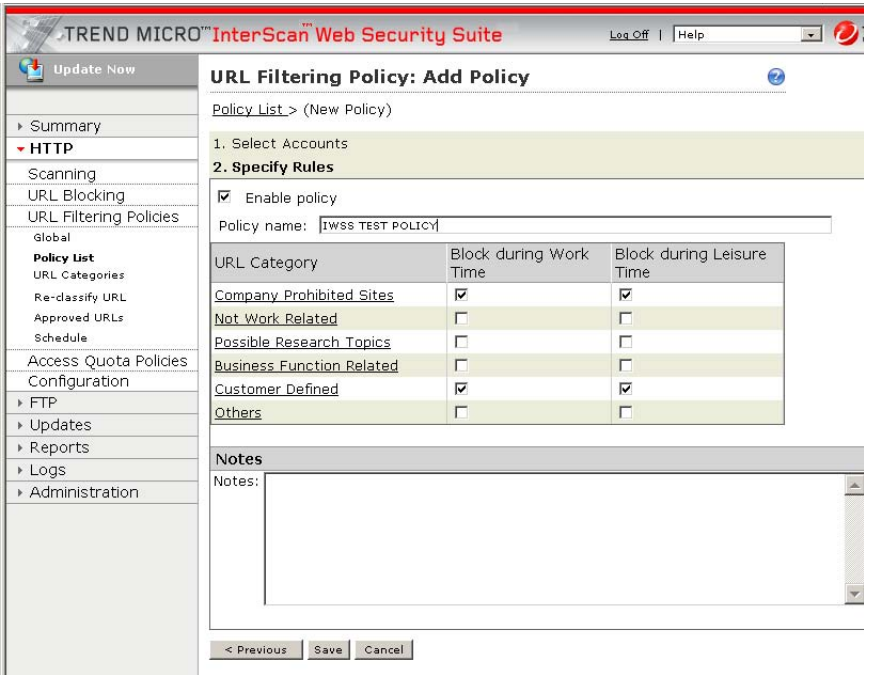


FIGURE 5-4. The "URL Filtering Policy: Add Policy" page.

7. Click **Save**.
8. In the **URL Filtering Policy List** screen, set the priority of the new policy (under the **Priority** column) by clicking on the up or down arrows.

Note: The **Priority** setting resolves the issue on what policy must be applied if there are accounts belonging to two or more policies.

9. Click **Save**.

FIGURE 5-5. Click "Deploy Policies" to implement the policy sooner than the set TTL value.

Modifying an Existing Policy

Any existing policy can be modified to better suit the current environment. You can also delete unnecessary policies by selecting the corresponding check box(es) and clicking **Delete Selected Line**.

To edit an existing policy:

1. Open the IWSS console and click **HTTP > URL Filtering Policies > Policy List**.
2. Click the link of the policy to be modified under **Policy**. The **URL Filtering Policy: Edit Policy** screen appears.
3. Under the **Rule** tab, make sure that **Enable policy** is selected.

   Select the URL Categories to be blocked during work and leisure time:

   - Company Prohibited Sites
   - Not Work Related
   - Possible Research Topics
   - Business Function Related
   - Customer Defined

- Others

Click **Save**.

4. Under the **Account** tab, configure the account settings, and then click **Save**.
5. To change the priority of the policy, go to **HTTP** > **URL Filtering Policies** > **Policy List**, and then set the priority of the edited policy (under **Priority**). Click the up arrow to increase the priority number, or click the down arrow to decrease priority.

Note: The **Priority** setting determines which policy is applied if there are accounts belonging to two or more policies.

6. Click **Save**.

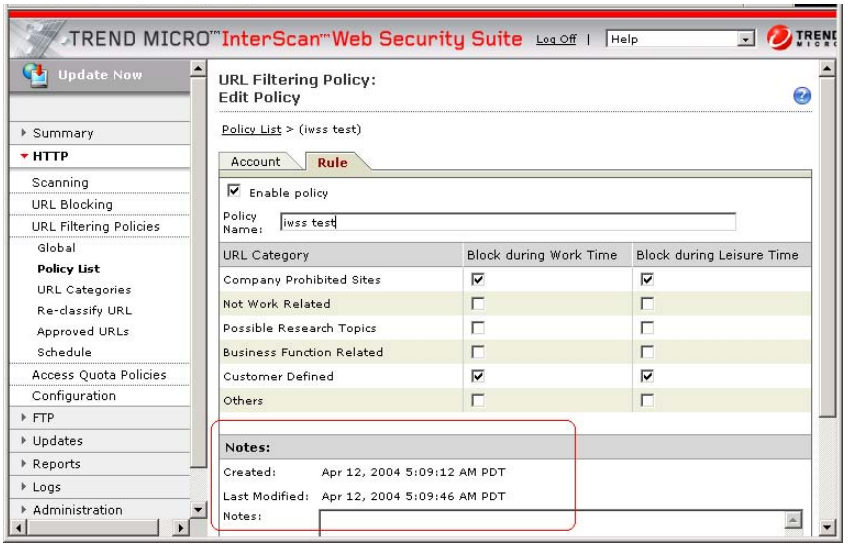


FIGURE 5-6. Use the "Notes" field to include valuable comments for a given policy.

Configuring the URL Filtering Approved List

IWSS gives you the option to set trusted sites (for example, your corporate internal Web sites) not to undergo URL filtering to prevent unnecessary overhead. You can add these trusted sites to the URL Filtering Approved List. These URLs are no longer classified and will not be accessible to the Web site for classification. Trend Micro recommends that you add all internal sites or other company approved URL sites to the **Do not filter the following sites** text box under **HTTP > URL Filtering Policies > Approved URLs**.

To configure the URL filtering approved list:

1. Open the IWSS console and click **HTTP > URL Filtering Policies > Approved URLs**.
2. In the **URL Filtering Approved List** screen, type the full Web address, URL keyword, or exact-match string in the **Match** field. Identify this entry by selecting one of the three options:
   - Web site
   - URL keyword
   - String

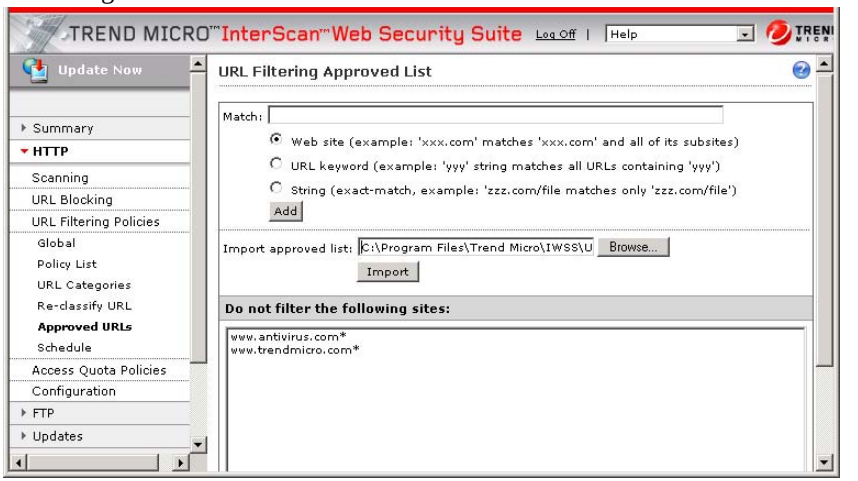


FIGURE 5-7. To import a file, write "URL Blocking Import File" on the first line of a file that contains a list of Web sites, URL keywords, or strings, and then write one rule per line.

3. Click **Add** to include this entry in **Do not filter the following sites**.

   Click **Remove** to remove highlighted entries from the list (or **Remove All** to remove all entries).
   To import a list of Web sites and URL strings from a given file to **Do not filter the following sites**, specify the location of the file in the **Import approved list** field by clicking **Browse**, and then click **Import**.

Note: Format the text file as follows:
line 1 = URL Blocking Import File
line 2 = [allow]
line 3 and so on: Type Web site, keyword, or string entry
For example:

```
URL Blocking Import File
[allow]
www.trendmicro.com*
www.antivirus.com*
```

---

4. Click **Save**.

Configuring Work Time Settings

IWSS uses the following default work time settings:

- Work days: from Monday to Friday
- Work hours: from 8:00 to 11:59 AM and 1:00 to 5:00 PM.

The time not designated as work time is considered as leisure time.

As different companies have varying work time schedules, IWSS gives you the option to configure the work time setting that is suitable to your environment.

To configure the URL filtering policy schedule:

1. Open the IWSS console and click **HTTP > URL Filtering Policies > Schedule**.
2. Under **Work Time Settings**, select the work days and work hours in the fields provided.

Note: It is assumed that all IWSS servers in a cluster are within the same time zone.

3. Click **Save**.

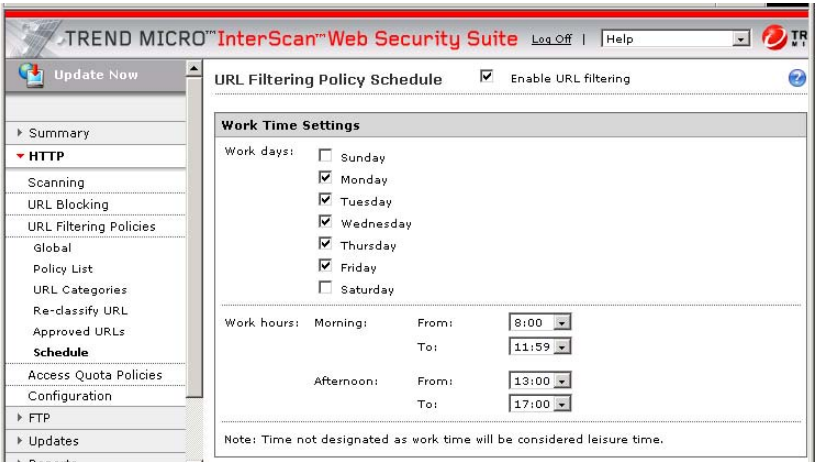


FIGURE 5-8. The time not designated as work time will be considered as leisure time.

Requesting URL Classification Review

For misclassified URLs, IWSS gives you the option to send these URLs to TrendLabs (see *TrendLabs* starting on page 10-9 for more details) for classification review.

To request URL classification review:

1. Open the IWSS console and click **HTTP > URL Filtering Policies > Re-classify URL**.
2. Under **Submit URL to TrendLabs for re-classification**, type the URL that you want to request a classification review by TrendLabs in the URL field provided. Also type your email address and notes in the fields provided. Make sure that the email server configuration is correct for this message to reach TrendLabs.

3. Click **Submit**.

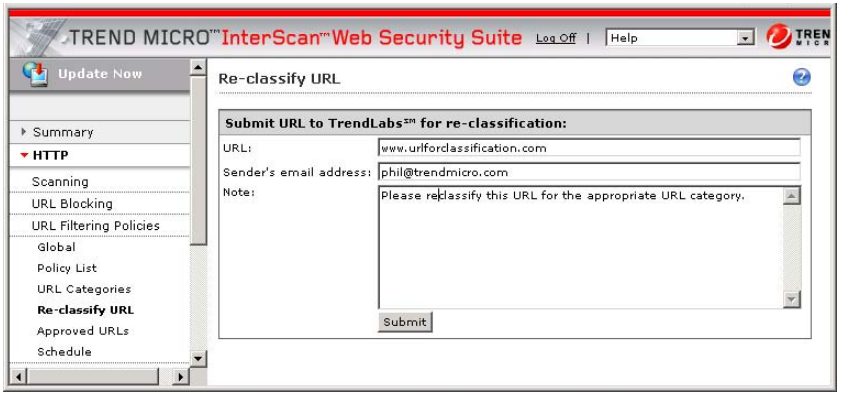


FIGURE 5-9. Provide a short description in the "Note" field of the URL being submitted for classification review.

Regrouping Categories

A default policy prevents access to a configurable set of category groups. You need to create additional policies to allow access to restricted category groups, that is for users that require broader access to the Internet because of their work functions. By doing so, you may need to regroup sub-categories belonging to some URL categories. For example, Travel, Restaurants/Dining/Food, Art/Entertainment are sub-categories defined by default under **Not Work Related**. These sub-categories, however, can be regrouped into a different category such as **Business Function Related**.

To regroup URL categories:

1. Open the IWSS console and click **HTTP > URL Filtering Policies > URL Categories**.
2. On the **URL Filtering Policies** screen, select the sub-category that you want to move to a new group.
3. Under **Move selected sub-categories to**, select the appropriate category from the drop-down menu.
4. Click **Save**.

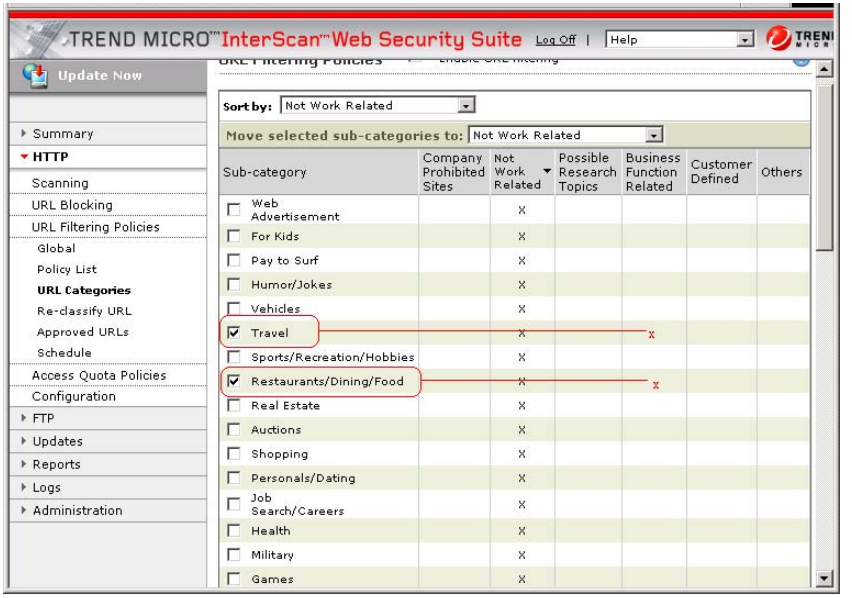


FIGURE 5-10. Select the new group from the "Move selected sub-categories to" drop-down menu.

Chapter 6

FTP Scanning

After installing the FTP service, configure IWSS for FTP scanning. Trend Micro recommends the following:

1. Update the virus pattern file and scan engine.
2. Enable FTP scanning.
3. Specify file types to block.
4. Specify file types to scan.
5. Configure compressed file scanning limits.
6. Configure scan actions on viruses.
7. Configure notifications.
8. Configure timeout settings.
9. Configure child processes.

Turning On/Off the FTP Service

Open the console and click **Summary** in the left menu. Click **Turn On** or **Turn Off** (at the top of the screen) to run or stop the FTP traffic, respectively. **Turn Off** means that the FTP service on the IWSS server is shut down, thus, a client cannot connect to the FTP server through the IWSS FTP proxy. The default setting is **On**.

Enabling FTP Scanning

You can enable or disable FTP scanning using the IWSS console. There are three FTP settings (stand-alone, local FTP, or FTP proxy) to choose from depending on your topology.

To enable or disable FTP scanning:

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

To configure proxy settings:

1. Open the IWSS console and click **FTP > Configuration**.
2. Under **Proxy Settings**, select the appropriate FTP setting based on your topology (see *FTP Installation Topology* starting on page 2-13 for the details of the settings available for FTP):
   - **Use stand-alone mode (logon = user@host)** — See *Testing FTP Scanning* starting on page 3-26 for more information on end-user instructions on how to download (Get) or upload (Put) any content via FTP
   - **Local FTP server location** — The FTP daemon can also act as a sentry standing guard for the local FTP server to handle FTP traffic (you need to specify the path or location of the FTP daemon)

- **Use FTP Proxy** — The FTP service works with an existing FTP proxy (you need to specify the host name of the server and port number)

FIGURE 6-1. The FTP Configuration page.

3. Click **Save**.

Specifying File Types to Block

You can identify the types of files that you want to block for security, monitoring or performance purposes. You can block file types such as Java applets, Microsoft Office documents, audio/video files, executables, and images.

To select which file types to block:

1. Open the IWSS console and click **FTP > Scanning** > **Target**.
2. Under the **Block these file types** section, select the file types to be blocked.
3. In the **Other file types** field, type other file types that you want to block (use a space to delimit multiple entries). See *Mapping File Types to Block with MIME Content-types* starting on page B-1 for the list of other file types to block.
4. Click **Save**.

Specifying File Types to Scan

IWSS scans all files, file types known to potentially harbor viruses (using IntelliScan to determine the true file type), or specified file types for viruses, including the individual files contained in a compressed file.

To select which file types to scan:

1. Open the IWSS console and click **FTP > Scanning** > **Target**.
   - To scan all file types regardless of extension, click **All file types** under **Scan these file types (if not blocked)**. IWSS opens compressed files and scans all files within. Scan all files is the most secure configuration.
   - To use true file type identification, click **IntelliScan** under **Scan these file types (if not blocked)**. IntelliScan is an intelligent scanning method, which uses a combination of true attachment type scanning and exact extension name scanning. True attachment type scanning recognizes the file type even if the file extension has been changed. IntelliScan automatically determines which scanning method to use.
   - You can skip files based on their extensions to work around performance issues. However, this is an unsafe practice, because the extension of a file is not a reliable means of determining its content, and viruses can exploit this vulnerability.

     To scan only selected file types, click **Specified file extensions** under **Scan these file types (if not blocked)**. This contains the list of known file types that harbor viruses. IWSS scans only those file types that are explicitly specified in the **Default Extensions** list and in the **Additional Extensions** text box.

     Use this option, for example, to decrease the aggregate number of files IWSS checks; thus, decreasing overall scan times.

   Note: There is no limit to the number or types of files you can specify. Do not precede an extension with the (*) character. Delimit multiple entries with a semicolon.

2. Click **Save**.

Default Extensions

These recommended extensions are activated by default and are updated with each new pattern file. The following extensions (current as of June 2004) are known file types that can potentially harbor viruses:

```
"";ARJ;BAT;BIN;BOO;CAB;CHM;CLA;CLASS;COM;CSC;DAT;DLL;DOC;DOT;DRV;EM
L;EXE;GZ;HLP;HTA;HTM;HTML;HTT;INI;JAR;JS;JSE;LNK;LZH;MDB;MPD;MPP;MP
T;MSG;MSO;NWS;OCX;OFT;OVL;PDF;PHP;PIF;PL;POT;PPS;PPT;PRC;RAR;REG;RT
F;SCR;SHS;SYS;TAR;VBE;VBS;VSD;VSS;VST;VXD;WML;WSF;XLA;XLS;XLT;XML;Z
;ZIP;{*;
```

Priority for FTP Scan Configuration

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

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

Configuring Compressed File Scanning Limits

IWSS opens and examines the contents of compressed files according to the criteria specified in the configuration screen (**FTP > Scanning > Target**). IWSS decompresses the files for scanning according to the configurable limits (number of files, decompressed file size, decompression ratio, and decompression layers).

To configure the compressed file scanning limits:

1. Open the IWSS console and click **FTP > Scanning > Target**.
2. Under **Compressed file handling**, select from the following two options:
   - **Block all compressed files**
   - **Scan compressed files within the limits**
     If you enable **Scan compressed files within the limits**, type a value for the following parameters:
     - Number of files (default is 10000)
     - Decompressed file sizes (default is 200MB)
     - Decompression percent (1-100) (default is 100)
     - Decompression layers (0-20) (default is 10)

3. Click **Save**.

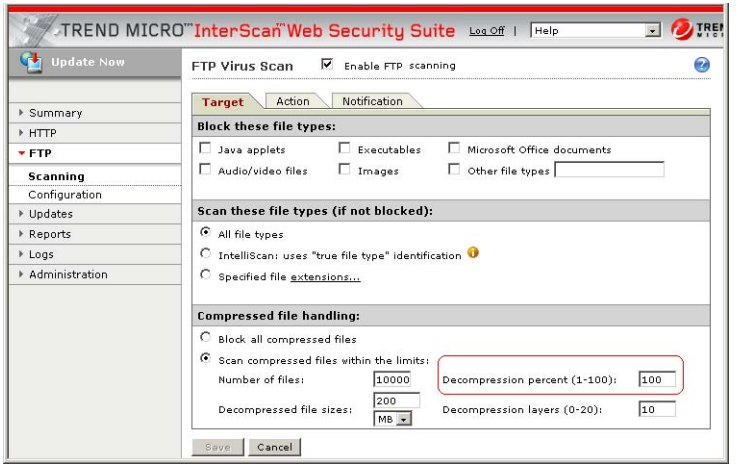


FIGURE 6-2. FTP Virus Scan page.

Note: "100" percent file decompression ratio means that there is no limit on the compressed files setting; whereas, "0" percent file decompression ratio means that all compressed files will be blocked.

Setting Scan Actions on Viruses

See *To set the FTP scan actions:* starting on page 6-8 for the procedure to set an action to be taken when a virus is detected. You can specify the action for FTP scanning to take upon finding an infected file (the recommended action setting is **Clean**):

- Choose **Quarantine** to move an infected file to the quarantine directory without cleaning. The requesting client will not receive the file.
- Choose **Delete** to delete an infected file at the server. The requesting client will not receive the file.
- Choose **Clean** to automatically clean and process an infected file. The requesting client will receive the cleaned file if it is cleanable.

You can specify the action for FTP scanning to take upon finding an uncleanable file, which includes worms and Trojans (the recommended action setting is **Delete**):

- Choose **Pass** to send an uncleanable file to the client without cleaning (Trend Micro does not recommend this choice, because it may allow infected files into your network).
- Choose **Quarantine** to move, without cleaning, an uncleanable file to the quarantine directory. The requesting client will not receive the file.
- Choose **Delete** to delete an uncleanable file at the server. The requesting client will not receive the file.

You can specify the action for FTP scanning to take in handling a password-protected compressed file (the recommended action setting is **Pass**):

- Choose **Pass** to send a password-protected file to the client without cleaning.
- Choose **Quarantine** to move a password-protected file to the quarantine directory. The requesting client will not receive the file.
- Choose **Delete** to delete a password-protected file at the server. The requesting client will not receive the file.

FIGURE 6-3. By default, the scan action settings for FTP scanning are: Clean for infected files; Delete for uncleanable files; and Pass for both password-protected compressed files and macros.

Macro Scan

Macro Scan detects macros in files during FTP transfers and provides scanning options (the recommended action setting is **Pass**).

- Choose **Quarantine** to move the files containing macro(s) to the quarantine directory.
- Choose **Clean** to remove macros before delivering the file.
- Choose **Pass** to disable special handling of files containing macro(s).

To set the FTP scan actions:

1. Open the IWSS console and click **FTP > Scanning > Action**.
2. Select the action for the following files:
   - Infected files (Delete, Quarantine, Clean)
   - Uncleanable files (Delete, Quarantine, Pass)
   - Password-protected files (Delete, Quarantine, Pass)
   - Macros (Quarantine, Clean, Pass)
3. Click **Save**.

Setting Virus Notification

When IWSS detects malicious code in a user's FTP transfer, IWSS can automatically send a customized email message to designated email addresses. You can configure the notification messages under **FTP > Scanning > Notification**.

To configure the notification settings:

1. Open the IWSS console and click **FTP > Scanning > Notification**.
2. Enable **Send a message when malicious code is found**. Select this option to have IWSS send a message via email to the administrator and/or designated others whenever a virus is detected in client FTP traffic. IWSS supports the following variables in this field:
   - %s -- name of detected threat
   - %d -- time and date of occurrence
   - %F -- file name (if any)
   - %a -- action taken

- %v -- name of detected threat

3. Configure the email settings by clicking  . Type a value for each configuration field:
   - Email address of the receiver of the notification messages in the **To address(es)** 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(es)** field
   - Domain name or the IP address of the mail server that will send the notification messages in the **Server name or IP address** field (the default is localhost)
   - Port used by the mail sever, typically 25, in the **SMTP server port** field
   - Frequency that the mail queue must be checked in the **Check mail queue in minutes** field
4. Click **Save**.

To display an additional message in the FTP client:

Select this option if you want to add a brief supplemental message to the automatic virus notification users see whenever IWSS detects that virus. The text message appears at the FTP command prompt; if the user is using a FTP client, the message will be displayed using whatever method the client software provides for session text.

1. Open the IWSS console and click **FTP > Scanning > Notification**.
2. Enable **Add additional message to your FTP prompt**. Type a message in the field provided.
3. Click **Save**.

Configuring Timeout Settings

This section describes how to configure client/server, write, and session timeout settings.

Client/server timeout settings

The client/server timeout setting indicates how long a client can be idle before stopping the connection. If the time of the request from client to server is longer than

the client/server timeout setting, the connection be closed. Thus, if the client or server does not respond in 120 seconds (default value), IWSS will close the connection. Use this feature to avoid waiting indefinitely for a reply from either a server or a client.

Write timeout

Write timeout affects how long data that is being sent can remain unconsumed, before the receiving client or server is presumed hung. If the response time from the server to the client is longer than the write timeout setting, the connection will be closed, thus, preventing further writing. The default value is 300 seconds.

Session timeout

The parent process regularly checks the connection status of child processes. If there is no response, then the child process will be stopped. The default setting is eight minutes.

Get and Put Mode

You can configure how IWSS behaves when sending (Put) and receiving (Get) files via FTP (**FTP > Configuration > Proxy Settings > Operation Options**). How you set Get and Put depends on whether FTP is installed in stand-alone mode, as a sentry for the local server, or with an upstream proxy.

Get mode

Normal— IWSS performs virus scanning in a temporary (/tmp) directory. The temporary file accumulates the data for file transfer and is scanned before being relayed to the destination system.

Local—The files that are resident on the system where the FTP daemon (isftpd) runs are scanned in place (this option only applies when protecting the local FTP site). This is not valid in stand-alone and proxy modes.

Note: When you set **Get** mode to **Local** and enable **stand-alone mode (logon=user@host)** or **Use FTP proxy**, the IWSS FTP daemon automatically resets the internal value back to **Normal**. Therefore, the files being transferred will be scanned as **Normal**.

FIGURE 6-4. Get and Put mode settings.

Put mode

Normal — IWSS performs virus scanning in a temporary (`/tmp`) directory. The temporary file accumulates the data for the file transfer and is scanned before being relayed to the destination system.

Through— The system stores incoming data into a temporary file while performing the data transfer in parallel. During FTP transfer, IWSS handles files based on the configuration specified on the configuration screen. You can define the actions the system needs to perform when it encounters a specific type of file:

- **Infected files**—available actions are **Delete**, **Quarantine**, **Clean**
- **Uncleanable files**—available actions are **Delete**, **Quarantine**, **Pass**
- **Password-protected files**—available actions are **Delete**, **Quarantine**, **Pass**
- **Macros**—available actions are **Quarantine**, **Clean**, **Pass**

Local—The files that are resident on the system where the FTP daemon (isftpd) runs on are scanned in place (this option only applies when protecting the local FTP site). This is not valid with stand-alone and proxy modes.

Note: When you set **Put** mode to **Local** and enable **stand-alone mode (Logon=user@host)** or **Use FTP proxy**, the IWSS FTP daemon automatically resets the internal value back to **Through**. Therefore, the files being transferred will be scanned as **Through**.

Configuring Child Processes

You can fine-tune the performance of IWSS by adjusting settings (**FTP > Configuration > Child Processes**) such as the number of processes spawned upon startup and the refresh rate of idle processes . In addition, you can limit the total number of child processes IWSS will use at any one time, and the total number of threads created for a given child process. Improperly adjusting the advanced settings can result in system instability. We recommend that you use the defaults unless there is a specific reason to alter them.

Pre-spawning processes

The IWSS FTP daemon, by default, creates one child process to handle the traffic load. Depending on your system resources and traffic load levels, you may want to increase the value in the **Number of pre-spawned processes** field. There is no

limitation on the number of child processes to be created. However, entering too high a value can result in wasted system resources.

FIGURE 6-5. Child Processes configuration page.

Regenerating idle processes

IWSS will automatically generate child processes as needed to accommodate traffic spikes. As traffic slows, excess child processes are left idle. You can specify, in seconds, how quickly these idle processes are stopped in the **Restart child processes after idling for** field.

Choosing the right idle time is important. The accumulation of many idle child processes means system resources are being wasted. On the other hand, existing idle processes can respond more rapidly to sudden increases in the workload than spawning new processes to accommodate the additional load.

- A typical number is 3600 seconds for **Restart child processes after idling for**.
- A **Restart child processes after idling for** value of zero means the number of available processes will always equal your highest usage spikes, no matter how brief or infrequent they may be. The idle child processes will never stop when you specify a value of zero (0).
- A **Restart child processes after idling for** value of just a few seconds means IWSS will have to create new processes just about every time there is a change in the workload.

In specifying a **Restart child processes after idling for** value, choose a number that represents a balance between the need to create new processes and the unwanted accumulation of idle processes.

Limiting child processes

Before creating a new child process, IWSS checks first to see if there are any existing processes that can be used. If there are none, IWSS will create a new one. Although there is typically no need to limit the number of child processes IWSS can create, this option allows you to set a maximum under the **Maximum number of simultaneous child processes** field. IWSS stops creating new processes whenever the maximum number of child processes is reached.

Extinguishing old connections

As a matter of "good housekeeping," IWSS FTP stops child processes after a set number of connections has been handled. This ensures that idle resources do not inadvertently remain active. A typical number to enter in the **Maximum connections for each child process before restart** field is 500, meaning that after 500 FTP connections have been handled, the hosting child process itself is terminated and a new one generated (a new child is only created if needed). This means that the child process is gone after serving the 500 connections. Setting this number too low can result in needlessly brief cycles. Enter a zero (0) in this field to disable the maximum number of connection options. The default value is 500.

Selecting how many threads to create

You have the option of selecting how many threads to create for each child process in the **Maximum number of threads to create for each child process** field. A typical maximum is five. Entering too high a number can contribute to system instability.

Chapter 7

Managing Logs

There are two types of logs available with IWSS: Reporting Logs and System Logs. There are multiple logs for each: HTTP scan, FTP scan, Mail delivery service, Administration, and Update logs are examples of system logs; and Virus, Spyware/Grayware, URL blocking, Performance, FTP, and URL access logs are examples of reporting logs.

System logs contain unstructured messages due to errors or state changes in the software, and are only visible by viewing the log file— they cannot be seen from the Web console. Reporting logs provide program event information, and can be seen in the IWSS console. The log data is stored in a database. It may optionally also be stored in text log files for compatibility with scripts the customer may have written, or as a redundant check to verify that the database is properly updated.

Topics included in this chapter are:

- Log File Naming Conventions
- Virus Log
- Spyware/Grayware Log
- URL Blocking Log
- URL Access Log
- Performance Log
- FTP Get Log

- FTP Put Log
- Deleting Report Logs
- Log Settings

Log File Naming Conventions

By default, log files are written to the `/etc/iscan` directory. The naming convention for log files, for example, is:

```
virus.log.2004.08.14
```

which can be read as [virus log name] for August 14, 2004

The naming conventions for each type of log are summarized in the following table:

TABLE 7-1. Log files naming conventions

Virus Log	`virus.log.yyyy.mm.dd`
URL Blocking	`url_blocking.log.yyyy.mm.dd`
Performance Log	`perf.log.yyyy.mm.dd`
URL Access Log	`access.log.yyyy.mm.dd`
FTP Log	`ftp.log.yyyymmdd.0001`
HTTP Log	`http.log.yyyym-mdd.0001`
Mail Delivery Log	`mail.log.yyyym-mdd.0001`
Update Log	`update.log.yyyym-mdd.0001`

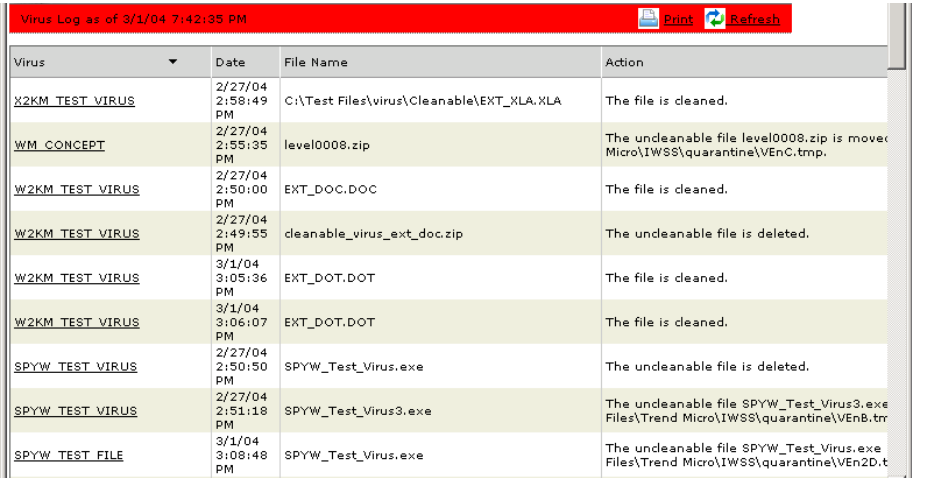
Virus Log

The virus log contains information on virus name, date and time of detection, name of the affected file, action taken, user ID, and scan type.

To view the virus log:

1. Open the IWSS console and click **Logs > Virus Log** in the left menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to view the virus log in a given time range, and then indicate the start and end dates.
3. Under **Viruses**, select virus(es) in the left list box to be added in the right list box. Highlight virus(es) to add, and then click **Add** (or **Add All** for all viruses listed). To remove virus(es) from the right list box, highlight the virus name(s) and click **Remove** (or **Remove All** for all viruses listed).
4. Under the **Sort by** section, select the appropriate option to sort the display log (Virus, Date, Action, Scan Type, File Name, User ID).
5. Click **Show Log**. The **Virus Log** viewing screen appears.



Virus	Date	File Name	Action
X2KM_TEST_VIRUS	2/27/04 2:58:49 PM	C:\Test Files\virus\Cleanable\EXT_XLA.XLA	The file is cleaned.
WM_CONCEPT	2/27/04 2:55:35 PM	level0008.zip	The uncleanable file level0008.zip is move Micro\IWSS\quarantine\VEnC.tmp.
W2KM_TEST_VIRUS	2/27/04 2:50:00 PM	EXT_DOC.DOC	The file is cleaned.
W2KM_TEST_VIRUS	2/27/04 2:49:55 PM	cleanable_virus_ext_doc.zip	The uncleanable file is deleted.
W2KM_TEST_VIRUS	3/1/04 3:05:36 PM	EXT_DOT.DOT	The file is cleaned.
W2KM_TEST_VIRUS	3/1/04 3:06:07 PM	EXT_DOT.DOT	The file is cleaned.
SPYW_TEST_VIRUS	2/27/04 2:50:50 PM	SPYW_Test_Virus.exe	The uncleanable file is deleted.
SPYW_TEST_VIRUS	2/27/04 2:51:18 PM	SPYW_Test_Virus3.exe	The uncleanable file SPYW_Test_Virus3.exe Files\Trend Micro\IWSS\quarantine\VEnB.tm
SPYW_TEST_FILE	3/1/04 3:08:48 PM	SPYW_Test_Virus.exe	The uncleanable file SPYW_Test_Virus.exe Files\Trend Micro\IWSS\quarantine\VEn2D.t

FIGURE 7-1. Sort the Virus log according to Virus, Date, Action, Scan Type, File Name, or User ID.

6. Click **Refresh** to update the virus log.

Spyware/Grayware Log

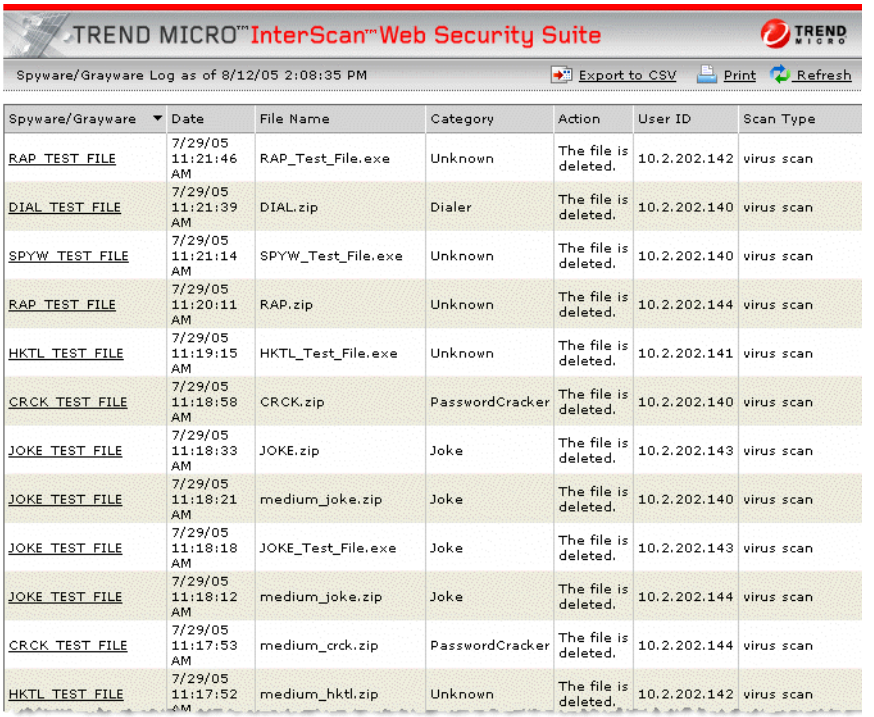
The Spyware/Grayware Log contains information on spyware and other grayware that has been detected in your network, including the name of the potential threat, the date and time of detection, the name of the file in which the threat was detected, the user ID of the user who encountered the threat, the category of threat (spyware, joke, dialer, and so on), and the action that was taken by IWSS (such as delete or quarantine).

To view the Spyware/Grayware log:

1. Open the IWSS console and click **Logs > Spyware/Grayware Log** in the left menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to view the URL blocking log in a given time range, and then indicate the start and end dates.
3. In the **Grayware** field, move the names of the grayware threats that you want to detect (shown in the left list box) to the right list box. To do so, highlight the grayware that you want to add, and then click **Add** (or **Add All** for all grayware listed). To remove the list of grayware from the right list box, highlight the grayware name(s) and then click **Remove** (or **Remove All** for all grayware listed).

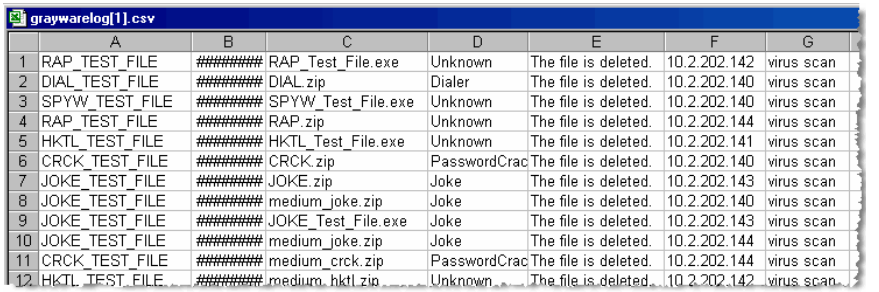
4. Click **Show Log**. The **Spyware/Grayware Log** viewing screen appears in a secondary browser window.



Spyware/Grayware	Date	File Name	Category	Action	User ID	Scan Type
RAP_TEST_FILE	7/29/05 11:21:46 AM	RAP_Test_File.exe	Unknown	The file is deleted.	10.2.202.142	virus scan
DIAL_TEST_FILE	7/29/05 11:21:39 AM	DIAL.zip	Dialer	The file is deleted.	10.2.202.140	virus scan
SPYW_TEST_FILE	7/29/05 11:21:14 AM	SPYW_Test_File.exe	Unknown	The file is deleted.	10.2.202.140	virus scan
RAP_TEST_FILE	7/29/05 11:20:11 AM	RAP.zip	Unknown	The file is deleted.	10.2.202.144	virus scan
HKTL_TEST_FILE	7/29/05 11:19:15 AM	HKTL_Test_File.exe	Unknown	The file is deleted.	10.2.202.141	virus scan
CRCK_TEST_FILE	7/29/05 11:18:58 AM	CRCK.zip	PasswordCracker	The file is deleted.	10.2.202.140	virus scan
JOKE_TEST_FILE	7/29/05 11:18:33 AM	JOKE.zip	Joke	The file is deleted.	10.2.202.143	virus scan
JOKE_TEST_FILE	7/29/05 11:18:21 AM	medium_joke.zip	Joke	The file is deleted.	10.2.202.140	virus scan
JOKE_TEST_FILE	7/29/05 11:18:18 AM	JOKE_Test_File.exe	Joke	The file is deleted.	10.2.202.143	virus scan
JOKE_TEST_FILE	7/29/05 11:18:12 AM	medium_joke.zip	Joke	The file is deleted.	10.2.202.144	virus scan
CRCK_TEST_FILE	7/29/05 11:17:53 AM	medium_crck.zip	PasswordCracker	The file is deleted.	10.2.202.144	virus scan
HKTL_TEST_FILE	7/29/05 11:17:52 AM	medium_hktl.zip	Unknown	The file is deleted.	10.2.202.142	virus scan

FIGURE 7-2. Sample spyware/ grayware log.

5. Click **Refresh** to update the Spyware/Grayware log. Click **Print** to print a copy of the log. Click **Export to CSV** to export the data to a .csv file. An example follows:



graywarelog[1].csv

	A	B	C	D	E	F	G
1	RAP_TEST_FILE	########	RAP_Test_File.exe	Unknown	The file is deleted.	10.2.202.142	virus scan
2	DIAL_TEST_FILE	########	DIAL.zip	Dialer	The file is deleted.	10.2.202.140	virus scan
3	SPYW_TEST_FILE	########	SPYW_Test_File.exe	Unknown	The file is deleted.	10.2.202.140	virus scan
4	RAP_TEST_FILE	########	RAP.zip	Unknown	The file is deleted.	10.2.202.144	virus scan
5	HKTL_TEST_FILE	########	HKTL_Test_File.exe	Unknown	The file is deleted.	10.2.202.141	virus scan
6	CRCK_TEST_FILE	########	CRCK.zip	PasswordCrac	The file is deleted.	10.2.202.140	virus scan
7	JOKE_TEST_FILE	########	JOKE.zip	Joke	The file is deleted.	10.2.202.143	virus scan
8	JOKE_TEST_FILE	########	medium_joke.zip	Joke	The file is deleted.	10.2.202.140	virus scan
9	JOKE_TEST_FILE	########	JOKE_Test_File.exe	Joke	The file is deleted.	10.2.202.143	virus scan
10	JOKE_TEST_FILE	########	medium_joke.zip	Joke	The file is deleted.	10.2.202.144	virus scan
11	CRCK_TEST_FILE	########	medium_crck.zip	PasswordCrac	The file is deleted.	10.2.202.144	virus scan
12	HKTL_TEST_FILE	########	medium_hktl.zip	Unknown	The file is deleted.	10.2.202.142	virus scan

FIGURE 7-3. Example of .csv file containing Spyware/Grayware log data.

URL Blocking Log

The URL blocking log contains information on URLs that have been blocked including the date and time blocking has occurred, category, blocking rule applied, user ID, Outbreak Prevention Policy (OPP) ID, scan type, and the full path of the URL that is blocked by IWSS.

To view the URL blocking log:

1. Open the IWSS console and click **Logs > URL Blocking Log** in the left menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days).

   Click **Range** to view the URL blocking log in a given time range, and then indicate the start and end dates.
3. Under **URLs blocked**, you can add the URL(s) listed in the left list box to the right list box. Highlight the URL(s) that you want to add, and then click **Add** (or **Add All** for all URLs listed). To remove the list of URLs from the right list box, highlight the URL(s) and then click **Remove** (or **Remove All** for all URLs listed).
4. Under **Sort by**, select the appropriate option to sort the display log.
   - **URL**—The URL address that is blocked
   - **Date**—The date and time when the file or URL is blocked

- **Category**—The rule defined by the user in the URL filtering policies, Access Quota, file blocking, PhishTrap, and URL blocking
- **Rule**—This is composed of the following:
  - IWSS-defined rule (block the URL containing a virus): displays the URL that has been blocked, for example
  - URL blocking rule: displays the URL in the block list, for example
  - URL filtering rule: displays the policy name, for example
  - OPP defined rule: displays the OPP rule, for example
  - File type defined rule: displays file block type, for example
  - PhishTrap defined rule: displays PhishTrap violation rule, for example
  - Access Quota defined rule: displays access quota violation rule, for example
- **OPP ID**—The ID number of the Outbreak Prevention Policy (OPP)
- **Scan Type**—For example, Normal, access quota, file type, URL memory block list, content filter, or PhishTrap.
- **User ID**—The IP address of the client machine where the browser resides, hostname, or user name

5. Click **Refresh** to update the URL blocking log.

Date	Category	Rule	User ID	Scan Type	OPP ID	Url
3/10/04 2:54:35 PM	Disease vector	PhishTrap	10.10.10.10	PhishTrap	0	http://ww2.coderz.net/kalamar/home.htm
3/10/04 2:54:53 PM	Malicious applet	PhishTrap	10.10.10.10	PhishTrap	0	http://www.yemp3.com/
3/10/04 2:58:59 PM	Malicious applet	PhishTrap	10.10.10.10	PhishTrap	0	http://www.yemp3.com/
3/10/04 2:58:57 PM	Malicious applet	PhishTrap	10.10.10.10	PhishTrap	0	http://www.yemp3.com/
3/10/04 2:58:53 PM	Malicious applet	PhishTrap	10.10.10.10	PhishTrap	0	http://www.yemp3.com/
3/10/04 3:18:42 PM	Malicious applet	PhishTrap	10.10.10.10	PhishTrap	0	http://www.yemp3.com/
3/10/04 2:58:10 PM	Malicious applet	PhishTrap	10.10.10.10	PhishTrap	0	http://www.waitsex.com/teen/
3/10/04 3:19:56 PM	Malicious applet	PhishTrap	10.10.10.10	PhishTrap	0	http://www.waitsex.com/teen
3/10/04 3:20:31 PM	Malicious applet	PhishTrap	10.10.10.10	PhishTrap	0	http://www.waitsex.com/teen
3/10/04 2:51:46 PM	work	www.example%2a.com*	10.10.10.10	normal	0	http://www.example*.com/
3/10/04 3:30:27 PM	Not Work Related	User Hsinghua	Hsinghua	content filter	0	http://www.aetv.com/
3/10/04 2:54:20 PM	Virus accomplice	PhishTrap	10.10.10.10	PhishTrap	0	http://www.achtungachtung.com/pup.exe
3/10/04 3:25:07 PM	Not Work Related	User Hsinghua	Hsinghua	content filter	0	http://www.a-blackjack-casino.com/
3/10/04 3:29:19 PM	Not Work Related	User Hsinghua	Hsinghua	content filter	0	http://www.a-blackjack-casino.com/
3/10/04 3:35:43 PM	Not Work Related	User Hsinghua	Hsinghua	content filter	0	http://www.a-blackjack-casino.com/
3/10/04 4:08:58 PM	Not Work Related	User Hsinghua	Hsinghua	content filter	0	http://www.a-blackjack-casino.com/
3/10/04 1:54:37 PM	work	10.2.202.177/virus/virus/noncleanable/ext_arj.arj	10.10.10.10	normal	0	http://10.2.202.177/virus/virus/NonCleanable/EXT
3/10/04 2:44:21 PM	work	COM file	10.10.10.10	normal	0	http://10.2.202.177/virus/NoVirus/COM_files/PKAR
3/10/04 1:56:53 PM	work	COM file	10.10.10.10	normal	0	http://10.2.202.177/virus/NoVirus/COM_files/ARC.
3/10/04 1:57:16 PM	work	COM file	10.10.10.10	normal	0	http://10.2.202.177/virus/NoVirus/COM_files/ARC.

FIGURE 7-4. Sample URL Blocking log.

Note: You can also find an entry in the **URL Blocking Log** when an FTP proxy blocks a file by type.

URL Access Log

The URL access log contains information on server name, date, user identification, client IP address, server IP address, domain, and path. IWSS records the URL access log only when **Log HTTP/FTP access events** is enabled (**Log HTTP/FTP access events** is disabled by default) under **Logs > Settings > Reporting Logs**. Each access monitoring record contains the following information:

- Date and time the access occurred
- User who visited the site
- IWSS server that processed the access
- IP address of the client system that made the request

Note: The network address translation may render this data meaningless, or at least make it appear that all requests are made from a single client.

- Domain accessed
- Path portion of the URL (the HTTP service can get the full URL path)
- IP address of the server from which the data was retrieved

To view the URL access log:

1. Open the IWSS console and click **Logs > URL Access Log** in the left menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days) from the drop-down menu.

   Click **Range** to view the URL access log in a given time range, and then indicate the start and end dates.

3. Under **Sort by**, select the appropriate option to sort the URL access log.
4. Click **Show Log**. The **URL Access Log** viewing screen appears.
5. Click **Refresh** to update the URL access log.

Server	Date	User ID	Client IP	Server IP	Domain	Path
QALAB-101-05	3/1/04 6:22:58 PM	Phil Monge	10.10.10.10	123.123.123.123	us.f105.mail.yahoo.com	ym/
QALAB-101-05	3/1/04 6:23:59 PM	Jet Matthew	10.10.10.12	123.123.123.123	us.f105.mail.yahoo.com	ym/
QALAB-101-05	3/1/04 6:24:27 PM	Phil Monge	10.10.10.10	123.123.123.123	us.f105.mail.yahoo.com	ym/
QALAB-101-05	3/1/04 6:21:13 PM	Jet Matthew	10.10.10.12	123.123.123.123	f105.mail.yahoo.com	ym/
QALAB-101-05	3/1/04 6:21:23 PM	Phil Monge	10.10.10.10	123.123.123.123	us.f105.mail.yahoo.com	ym/
QAL-101-04	2/27/04 3:04:54 PM	Kathy Q	10.10.10.11	123.123.123.123	us.f607.mail.yahoo.com	ym/
QAL-101-04	2/27/04 3:05:21 PM	Kathy Q	10.10.10.11	123.123.123.123	us.f607.mail.yahoo.com	ym/
QAL-101-04	2/27/04 3:05:10 PM	Kathy Q	10.10.10.11	123.123.123.123	us.f607.mail.yahoo.com	ym/
QAL-101-04	2/27/04 3:05:11 PM	Kathy Q	10.10.10.11	123.123.123.123	us.f607.mail.yahoo.com	ym/
	3/1/04					

FIGURE 7-5. Sort the URL Access log according to Server, Date, User, ClientIP, ServerIP, Domain, or Path.

Performance Log

The performance log contains information on server name, date, and the type and value of the performance metric. Each performance metric record contains the following information:

- Date and time the metric was recorded
- IWSS server that recorded the metric
- Metric name (one of: `HTTP Requests Processed, HTTP Responses Processed, Number of HTTP threads, HTTP CPU % Utilization`)

- Metric value

Server	Date	Matrix Name	Value
QALAB-101-05	3/1/04 11:42:29 AM	HTTP Requests Processed	0
QALAB-101-05	3/1/04 11:42:29 AM	HTTP Responses Processed	0
QALAB-101-05	3/1/04 11:42:29 AM	HTTP CPU % Utilization	10
QALAB-101-05	3/1/04 11:42:29 AM	Number of HTTP Threads	11
QALAB-101-05	3/1/04 11:43:33 AM	HTTP Requests Processed	0
QALAB-101-05	3/1/04 11:43:33 AM	HTTP Responses Processed	0
QALAB-101-05	3/1/04 11:43:33 AM	HTTP CPU % Utilization	0
QALAB-101-05	3/1/04 11:43:33 AM	Number of HTTP Threads	12
QALAB-101-05	3/1/04 11:46:33 AM	HTTP Requests Processed	0
QALAB-101-05	3/1/04 11:46:33 AM	HTTP Responses Processed	0
QALAB-101-05	3/1/04 11:46:33 AM	HTTP CPU % Utilization	0
QALAB-101-05	3/1/04 11:46:33 AM	Number of HTTP Threads	12
QALAB-101-05	3/1/04 11:49:33 AM	HTTP Requests Processed	0
QALAB-101-05	3/1/04 11:49:33 AM	HTTP Responses Processed	0
QALAB-101-05	3/1/04 11:49:33 AM	HTTP CPU % Utilization	0
QALAB-101-05	3/1/04 11:49:33 AM	Number of HTTP Threads	12
QALAB-101-05	3/1/04 11:52:33 AM	HTTP Requests Processed	0

FIGURE 7-6. Sample Performance log.

To view the performance log:

1. Open the IWSS console and click **Logs > Performance Log** in the left menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days) from the drop-down menu.

   Click **Range** to view the performance log in a given time range, and then indicate the start and end dates.
3. Under **Sort by**, select the appropriate option to sort the performance log.
4. Click **Show Log**. The **Performance Log** viewing screen appears.
5. Click **Refresh** to update the performance log.

FTP Get Log

The FTP Get log contains all FTP Get transaction information, which includes user name, date, FTP transfer source, and file name.

User ID	Date	From	File Name
administrator@123.123.123.123	2/27/04 3:49:40 PM	123.123.123.123	
administrator@123.123.123.123	2/27/04 3:50:47 PM	123.123.123.123	EXT_Z.Z
administrator@123.123.123.123	2/27/04 3:51:29 PM	123.123.123.123	EXT_PL.PL
administrator@123.123.123.123	2/27/04 3:51:37 PM	123.123.123.123	mp3-pwd.zip
administrator@123.123.123.123	2/27/04 3:51:38 PM	123.123.123.123	NonCleanable

FIGURE 7-7. Sort the FTP Get log according to User, Date, From, or File Name.

To view the FTP Get log:

1. Open the IWSS console and click **Logs > FTP Get Log** in the left menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days) from the drop-down menu.

   Click **Range** to view the FTP Get log in a given time range, and then indicate the start and end dates.
3. Under **Sort by**, select the appropriate option to sort the display log.
4. Click **Show Log**. The **FTP Get log** viewing screen appears.
5. Click **Refresh** to update the FTP Get log.

FTP Put Log

The FTP Put log contains all FTP Put transaction information, which includes user name, date, sender identification, and file name.

User ID	Date	From
p@123.123.123.123	2/24/04 4:59:00 PM	123.123.123.123
p@123.123.123.123	2/24/04 4:58:58 PM	123.123.123.123
p@123.123.123.123	2/24/04 4:58:55 PM	123.123.123.123

FIGURE 7-8. Sort the FTP Put log according to User, Date, From, or File Name.

To view the FTP Put log:

1. Open the IWSS console and click **Logs > FTP Put Log** in the left menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days) from the drop-down menu.

   Click **Range** to view the FTP Put log in a given time range, and then indicate the start and end dates.
3. Under **Sort by**, select the appropriate option to sort the display log.
4. Click **Show Log**. The **FTP Put Log** viewing screen appears.
5. Click **Refresh** to update the FTP Put log.

Deleting Report Logs

You can delete logs (log data in files) that are no longer needed from the directory of a given virus log, URL blocking log, URL access log or performance log.

Note: Deleting a log will not necessarily remove the corresponding data from a display in the IWSS console. You need to remove the corresponding data from the appropriate database table (see *Major database tables for IWSS logging/reporting.* starting on page 8-22 for more information).

To delete one or more logs:

1. Open the IWSS console and click **Logs > Deletion** in the left menu.
2. In the **Log File** column, select dates for which logs are to be deleted for the:
   - Virus Log (includes Get and Put logs)
   - URL Blocking Log
   - URL Access Log
   - Performance Log
3. Click **Delete**, and then confirm by clicking **OK** on the next screen.

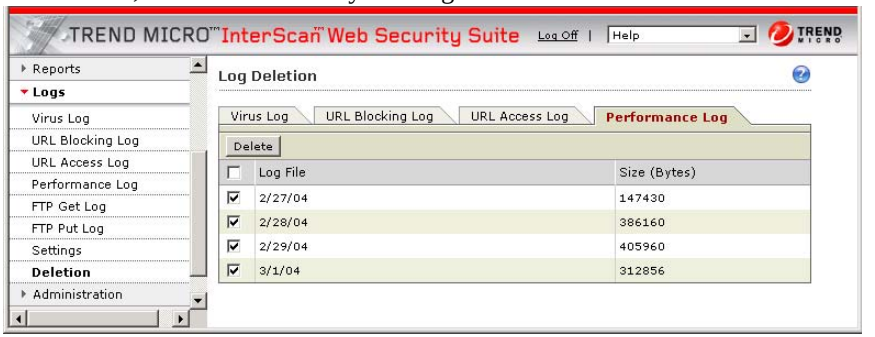


FIGURE 7-9. Summarize the log list according to date and size (in bytes).

Log Settings

On the **Log Settings** screen, you have the option to configure the following:

- Gather performance data
- Log HTTP/FTP access events
- Database log update interval
- Write logs to database and log files or database only
- Directories for reporting and system logs
- Number of days to keep the system logs
- Quarantine directory.

Directory Locations

You can configure the directories for the Reporting Log, System Log, and Quarantine. The default location is `/etc/iscan/log` for both reporting and system log directories and `/etc/iscan/quarantine` for the quarantine directory. IWSS checks if the directory entered exists on the IWSS server. If the directory is not on the

IWSS server, an error message will appear to notify you that the directory you entered is not accessible.

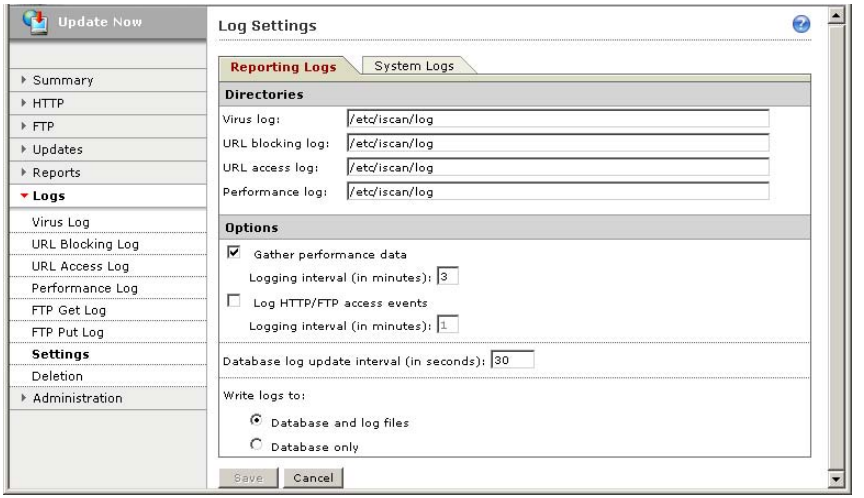


FIGURE 7-10. You have the option of writing logs to database and log files or database only.

To configure reporting log directories:

1. Open the IWSS console and click **Logs > Settings > Reporting Logs**.
2. In their corresponding text boxes, type the log directory of the following:
   - Virus log
   - URL blocking log
   - URL access log
   - Performance log
3. Click **Save**.

To configure the system log directories:

1. Open the IWSS console and click **Logs > Settings > System Logs**.
2. In their corresponding text boxes, type the log directory of the following:
   - HTTP scan log
   - FTP scan log
   - Mail delivery daemon log
   - Administration log
   - Update log
3. Click **Save**.

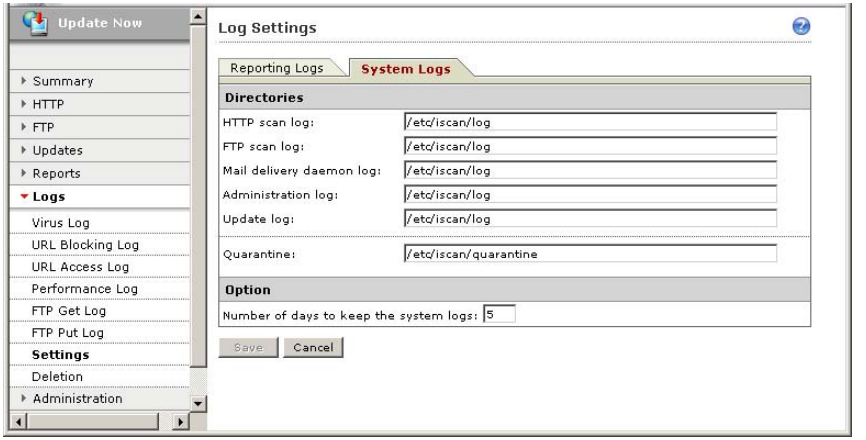


FIGURE 7-11. The default number of days to keep the system logs is 5.

To configure the quarantine directory:

1. Open the IWSS console and click **Logs > Settings > System Logs**.
2. Under **Quarantine**, type the folder where you want quarantined items to be copied.
3. Click **Save**.

Chapter 8

Managing Reports

IWSS provides you with statistics that are useful in generating reports for a long-term network traffic profile. These reports help you to optimize the network capability and its security. IWSS gives you the option of generating reports based on a given category of a specific user, all users, all groups or specific group(s). You can either create the report manually (real-time) or on a scheduled basis. A report notification can be sent to the email addresses defined in the configuration setting at given time intervals.

Topics included in this chapter are:

- Viewing the Threat Report
- Generating Reports
- Configuring Real-time Reports
- Configuring Scheduled Reports
- Importing Data

Viewing the Threat Report

When you first log on to IWSS, the **Summary** view is the default view that appears. Click the **Spyware** tab on the **Summary** view to see if any spyware or other grayware has been detected on your network today, during the past week, or during the past month. For example:

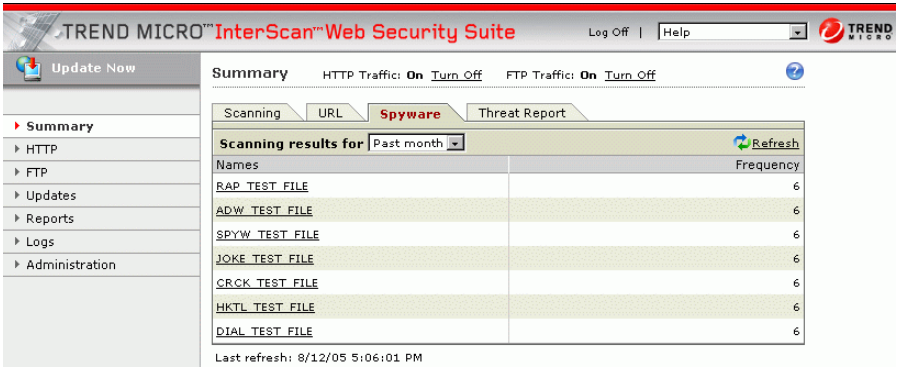


FIGURE 8-1. View spyware/grayware threats detected today, in the past week, or in the past month via the Spyware tab in the Summary view.

The **Spyware** tab allows you to view threats by name and frequency.

Click a specific threat name to open the Trend Micro Virus Encyclopedia search page, to get more information about a specific threat. The Virus Encyclopedia contains a description of all known spyware and other grayware, as well as viruses, Trojans, worms, and so on. The description includes risk ratings, as well as solutions, technical details, and statistics.

For example:

FIGURE 8-2. Sample of spyware information from the Trend Micro Virus Encyclopedia.

If spyware and other grayware is detected on the **Spyware** tab, click the **Threat Report** tab to see a detailed report of the threats. For example:

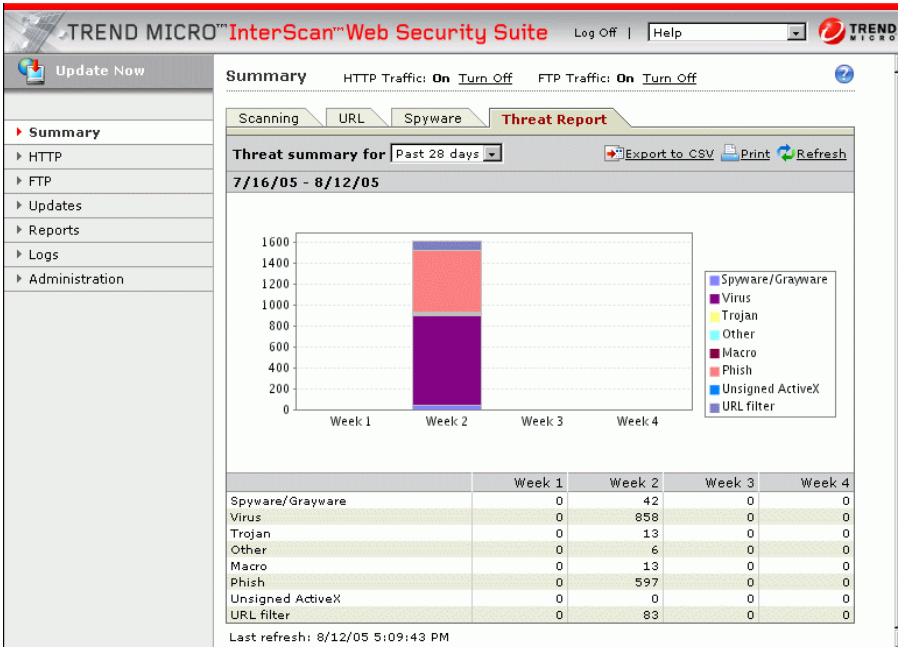


FIGURE 8-3. Sample of the Threat Report.

Generating Reports

IWSS gives you the option of writing the reporting logs to database and text files or to a database only. This option can be configured in the IWSS console under **Logs > Settings > Reporting Logs** (see *Log Settings* starting on page 7-15 for more information). The text logs are available for backward compatibility with IWSS 1.0 and to allow further analysis of log data through custom scripts or other third-party applications. They can also be used in validating the completeness and accuracy of logging to the database.

Note: For better performance, Trend Micro recommends that you migrate to "database only." Data for reports is recorded to the database at a configurable interval.

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 not enabled. Conversely, if IWSS is configured as an upstream proxy, valuable data on user activities may not be available to IWSS. Thus, you need to decide whether or not you want IWSS to be the mechanism to summarize all Web activities. If you do, then the access logging must be enabled under **Logs > Settings > Reporting Logs > Options**.

The IWSS console displays graphs and statistics for a generated report. Graphs can be displayed in various formats:

- Bar
- Stacked bar
- Line

Note: The IWSS package is bundled with PostgreSQL 7.4.1. IWSS also supports Oracle 8i/9i.

There are two types of report generated:

- Blocking event report
- Traffic report for URL filtering

You can view the following report categories for each type on the IWSS console or via Control Manager:

Blocking-event Reports

- Riskiest URLs by viruses detected
- Riskiest users by infected URLs accessed
- Most violations by user
- Most violations by group
- Most blocked URL categories
- Most blocked URLs

- Most blocked URLs by day of the week
- Most blocked URLs by hour

Traffic Reports

- Most active users
- Most popular URLs
- Most popular downloads
- Most popular search engines
- Daily traffic report
- Activity level by day of the week
- Activity level by hour
- Per user report

Spyware/Grayware Reports

- Spyware/grayware detections by category
- Top spyware/grayware detections
- Most detections by user

Configuring Real-time Reports

You can schedule IWSS to automatically create periodic reports in real time based on a given category of a specific user, all users, all groups or specific group(s) and send you the URL via email. You can also define and generate custom reports at any time from the **Real-time Reports** page by clicking **Generate Report** at the bottom of the page. Report content is affected by the User ID method you are using and the availability of logging data.

To configure real-time reports:

1. Open the IWSS console and click **Reports > Real-time Reports** in the left menu.
2. Under **Time period**, select a time (All Dates, Today, Last 7 days, Last 30 days) from the drop-down menu.

Click **Range** to generate a report in a given time range, and then indicate the start and end dates.

3. Under **Report by**, select one of the following four options:
   - All users
   - Specific user(s)
   - All groups
   - Specific group(s)
4. Under **Report Type**, select one of the two types of report to be generated
   - Consolidated report
   - Individual report - select from the listed reports
     - Blocking-event reports
     - Traffic reports
     - Spyware/Grayware reports
5. Under **Options**, select the following chart type from the drop-down menu:
   - Bar
   - Stacked bar
   - Line

   To distinguish blocked and unblocked traffic on a given chart, select **Distinguish blocked from unblocked traffic**. Choose this option to have IWSS break out user data in the report to show hits on blocked sites versus hits on unblocked sites. This option only applies if you will generate a Consolidated report or will include any individual reports for URL Blocking.

6. Click **Generate Report**.

TABLE 8-1. Relationship between Report by and Report Type

Report by	Report Type	
	Consolidated report	**Individual report**
All users	Includes all listed reports except for "Per user report"	"Per user report" is disabled
Specific users	"Per user report"	Only "Per user report" is enabled
All groups or Specific groups	Included are only these five reports: o Most violations by group· o Most blocked URL categories o Most blocked URLs o Most blocked URLs by day of the week o Most blocked URLs by hour	These five reports are enabled: o Most violations by group o Most blocked URL categories o Most blocked URLs o Most blocked URLs by day of the week o Most blocked URLs by hour

To select specific group(s):

1. Open the IWSS console and click **Reports > Real-time Reports** in the left menu.
2. Under **Report by**, select **Specific group(s)**, and then click **Select**.

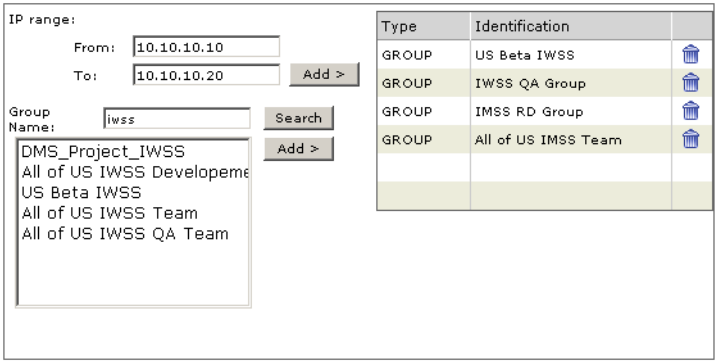


FIGURE 8-4. Select Groups page.

Note: When you click **Select** on **Specific group(s)** (**Reports > Real-time Reports > Report by**), the **Select Groups** pop-up screen displays according to the setting made in the user identification method (**HTTP > Configuration > User ID**).

---

3. Type the IP address range or type a group name in the fields provided.
4. Click **Add**.
5. Click **Save**

To select specific user(s):

1. Open the IWSS console and click **Reports > Real-time Reports** in the left menu.
2. Under **Report by**, select **Specific user(s)**, and then click **Select**.

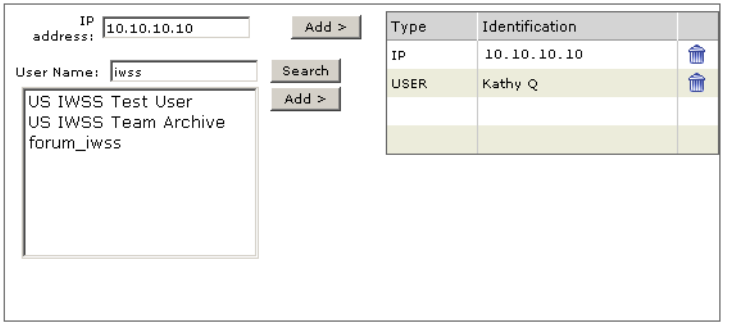
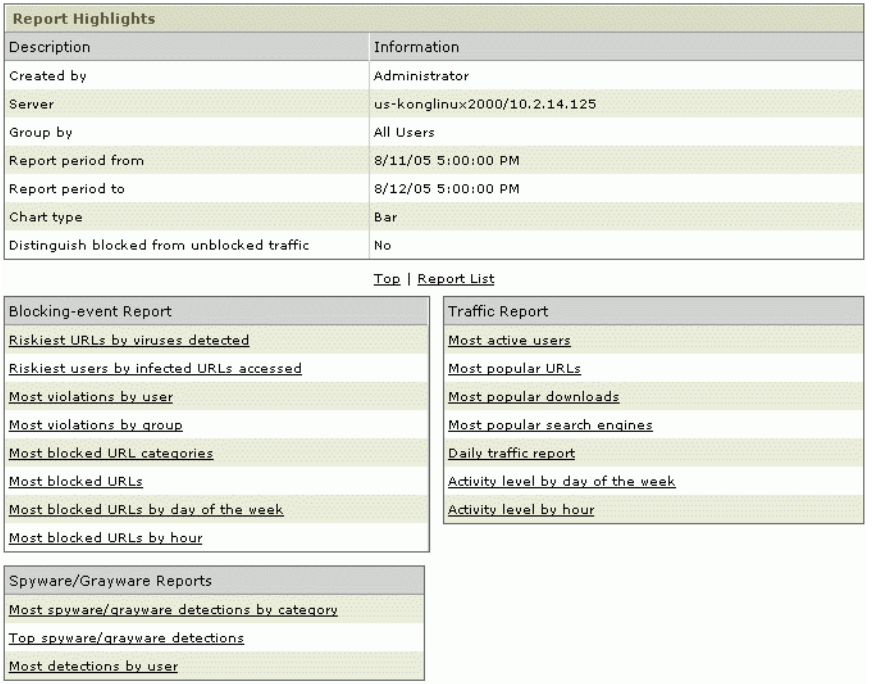


FIGURE 8-5. Select Users page.

Note: When you click **Select** on **Specific user(s)** (**Reports > Real-time Reports > Report by**), the **Select Users** pop-up screen displays according to the setting made in the user identification method (**HTTP > Configuration > User ID**).

3. Type the IP address or the user name in the fields provided.
4. Click **Add**.
5. Click **Save**



Report Highlights

Description	Information
Created by	Administrator
Server	us-konglinux2000/10.2.14.125
Group by	All Users
Report period from	8/11/05 5:00:00 PM
Report period to	8/12/05 5:00:00 PM
Chart type	Bar
Distinguish blocked from unblocked traffic	No

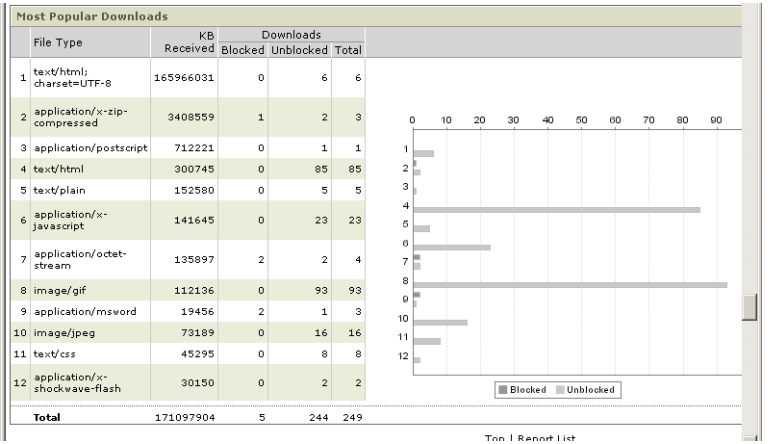
Top | Report List

Blocking-event Report
Riskiest URLs by viruses detected
Riskiest users by infected URLs accessed
Most violations by user
Most violations by group
Most blocked URL categories
Most blocked URLs
Most blocked URLs by day of the week
Most blocked URLs by hour

Traffic Report
Most active users
Most popular URLs
Most popular downloads
Most popular search engines
Daily traffic report
Activity level by day of the week
Activity level by hour

Spyware/Grayware Reports
Most spyware/grayware detections by category
Top spyware/grayware detections
Most detections by user

FIGURE 8-6. Real-time consolidated report highlights.

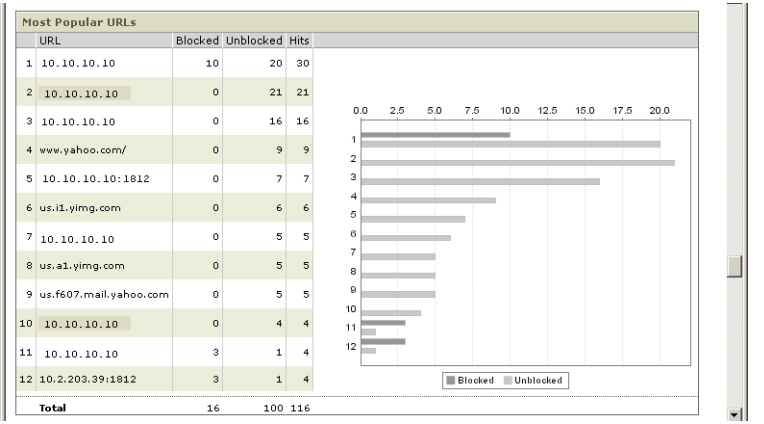


Most Popular Downloads

	File Type	KB Received	Downloads Blocked	Unblocked	Total
1	text/html; charset=UTF-8	165966031	0	6	6
2	application/x-zip-compressed	3408559	1	2	3
3	application/postscript	712221	0	1	1
4	text/html	300745	0	85	85
5	text/plain	152580	0	5	5
6	application/x-javascript	141645	0	23	23
7	application/octet-stream	135897	2	2	4
8	image/gif	112136	0	93	93
9	application/msword	19456	2	1	3
10	image/jpeg	73189	0	16	16
11	text/css	45295	0	8	8
12	application/x-shockwave-flash	30150	0	2	2
	Total	171097904	5	244	249

Top | Report List

FIGURE 8-7. "Most Popular Downloads" report with "Distinguish blocked from unblocked traffic" enabled.



Most Popular URLs

	URL	Blocked	Unblocked	Hits
1	10.10.10.10	10	20	30
2	10.10.10.10	0	21	21
3	10.10.10.10	0	16	16
4	www.yahoo.com/	0	9	9
5	10.10.10.10:1812	0	7	7
6	us.i1.yimg.com	0	6	6
7	10.10.10.10	0	5	5
8	us.a1.yimg.com	0	5	5
9	us.f607.mail.yahoo.com	0	5	5
10	10.10.10.10	0	4	4
11	10.10.10.10	3	1	4
12	10.2.203.39:1812	3	1	4
	Total	16	100	116

FIGURE 8-8. "Most Popular URLs" report with "Distinguish blocked from unblocked traffic" enabled.

Configuring Scheduled Reports

You can set IWSS to generate scheduled reports on a daily, weekly, or monthly basis. To control the large volume of reports generated, IWSS gives you the option to delete unnecessary scheduled reports. You can also customize the number of records (for example, URLs, users, violations) of the following reports, which is configurable under **Reports > Settings > Customization**:

Blocking-event reports:

- Riskiest URLs by viruses detected
- Riskiest users by infected URLs accessed
- Most violations by user
- Most violations by group
- Most blocked URL categories
- Most blocked URLs

Traffic reports:

- Most active users
- Most popular URLs
- Most popular downloads
- Most popular search engines

Note: Group report gives you the blocking events that are triggered by a policy for a group, not the activities of members of that group in general.

- Most popular search engines

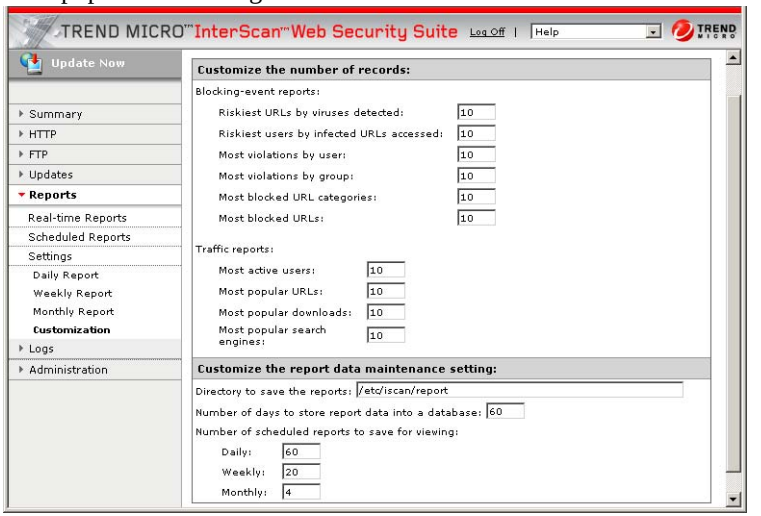


FIGURE 8-9. By default, the data are stored in a database for 60 days.

To customize the report setting:

1. Open the IWSS console and click **Reports > Settings > Customization** in the left menu.
2. Under **Customize the number of records**, type the appropriate number of records for each report to be generated.
3. Under **Customize the report data maintenance setting**, type the following information in the fields provided:
   a. Directory to save the reports (the default is `/etc/iscan/report`)
   b. Number of days to store report data into a database (the default is 60 days)
   c. Number of scheduled reports to save for viewing:
      - Daily (the default is 60)
      - Weekly (the default is 20)
      - Monthly (the default is 4)
4. Click **Save**.

To configure daily reports:

1. Open the IWSS console and click **Reports > Settings > Daily Report** in the left menu.
2. Enable **Generate daily reports**, and then select a start time from the drop-down menu.
3. Type the email address(es) of the receiver(s) of the report notification in the **Send report notification to** field.
4. Under **Report by**, select one of the following four options:
   - All users
   - Specific user(s)
   - All groups
   - Specific group(s)
5. Under **Report Type**, select the type of report to be generated.
   - Consolidated report
   - Individual report
     - Blocking-event reports
     - Traffic reports
     - Spyware/grayware reports
6. Under **Options**, select the chart type from the drop-down menu (Bar, Stacked bar, or Line).

   To view the activity for both blocked and unblocked traffic on a given chart, select **Distinguish blocked from unblocked traffic**.

7. Click **Save**.

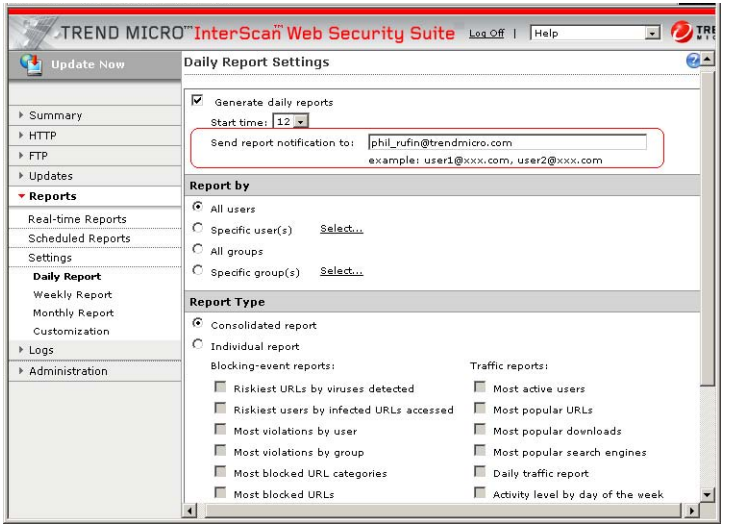


FIGURE 8-10. Delimit multiple email addresses with a comma.

To configure weekly reports:

1. Open the IWSS console and click **Reports > Settings > Weekly Report** in the left menu.
2. Enable **Generate weekly reports every**, select the day of the week and a start time from the drop-down menu.
3. Type the email address(es) of the receiver(s) of the report notification in the **Send report notification to** field.
4. Under **Report by**, select one of the following four options:
   - All users
   - Specific user(s)
   - All groups
   - Specific group(s)

5. Under **Report Type**, select one of the two types of report to be generated
   - Consolidated report
   - Individual report
     - Blocking-event reports
     - Traffic reports
     - Spyware/grayware reports
6. Under **Options**, select the chart type from the drop-down menu (Bar, Stacked bar, or Line).

   To view the activity for both blocked and unblocked traffic on a given chart, select **Distinguish blocked from unblocked traffic**.
7. Click **Save**.

FIGURE 8-11. "Generate weekly reports every Sunday" is enabled by default.

To configure monthly reports:

1. Open the IWSS console and click **Reports > Settings > Monthly Report** in the left menu.
2. Enable **Generate monthly reports on date**, select the date of the month and a start time from the drop-down menu.
3. Type the email address(es) of the receiver(s) of the report notification in the **Send report notification to** field.
4. Under **Report by**, select one of the following four options:
   - All users

- Specific user(s)
- All groups
- Specific group(s)

5. Under **Report Type**, select one of the two types of report to be generated
   - Consolidated report
   - Individual report
     - Blocking-event reports
     - Traffic reports
     - Spyware/grayware reports
6. Under **Options**, select the chart type from the drop-down menu (Bar, Stacked bar, or Line).

   To view the activity for both blocked and unblocked traffic on a given chart, select **Distinguish blocked from unblocked traffic**.
7. Click **Save**.

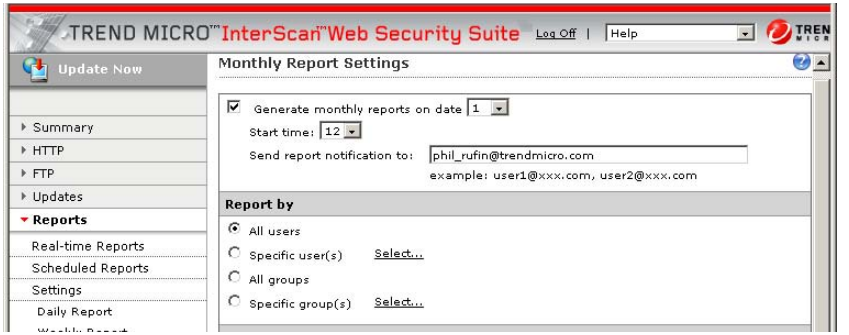


FIGURE 8-12. Monthly report setting page.

To delete scheduled reports:

1. Open the IWSS console and click **Reports > Scheduled Reports** in the left menu.
2. Select the reports (daily, weekly, or monthly) to be deleted.

3. Click **Delete** for selected individual report(s) (or **Delete All** for all the reports).

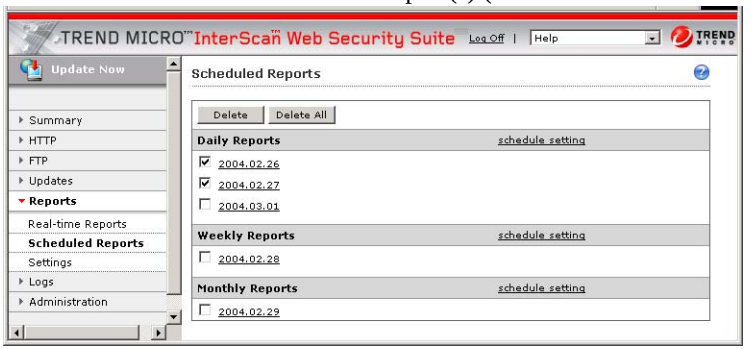


FIGURE 8-13. Click "schedule setting" to return to the report setting page.

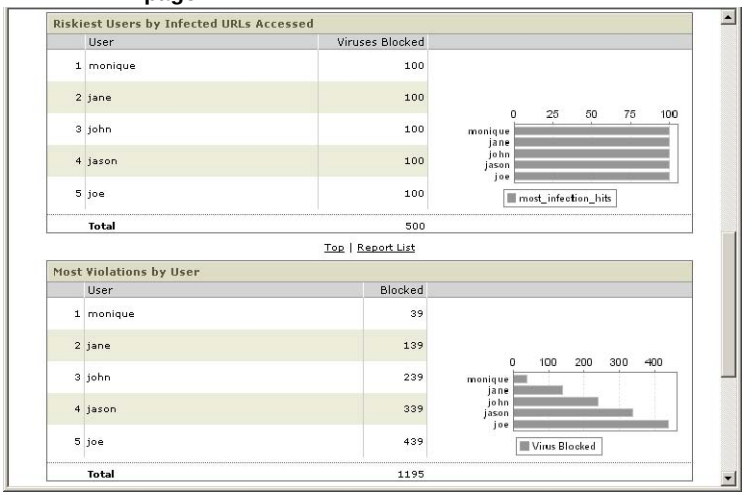


FIGURE 8-14. A sample daily report for all users, which shows "Riskiest Users by Infected URLs Accessed" and "Most Violations by User".

Importing Data

You can access information from the IWSS database using other third-party tools. The following example gives you the procedure of importing data using the Microsoft Excel application.

Note: Prior to using Microsoft Excel to query the PostgreSQL database, the windows ODBC driver for PostgreSql should be installed (the PostgreSql ODBC driver can be downloaded from `http://www.postgresql.org`). Likewise, the ODBC driver also needs to be installed if data querying is to be performed through Microsoft Excel or Access on MS Windows 2000. Please refer to Oracle's documentations for the Oracle ODBC driver installation.

To import data using the Microsoft Excel application:

1. Open Excel and click **Data > Get External Data > New Database Query**.
2. Under **Choose Data Source > Databases**, select the data source name (for example, **IWSS*)**. Click **OK**.

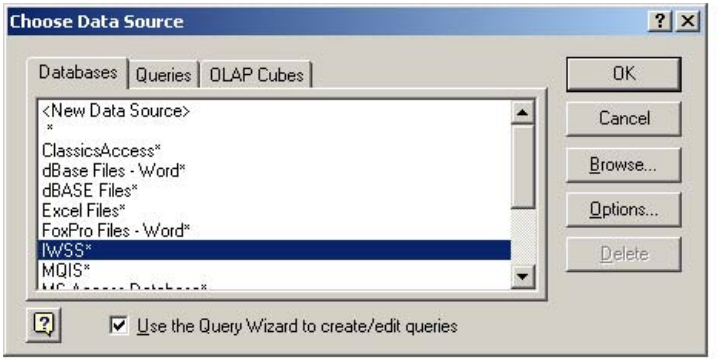


FIGURE 8-15. Choose Data Source screen.

3. Type your logon credentials in the next screen. Click **OK**.
4. In the **Available table and columns** field of the **Query Wizard - Choose Columns** screen, select `tb_url_usage`, and then add to the **Columns in your query** field. Click **Next**. Table 8-2 gives you a sample of major database tables for IWSS logging/reporting.

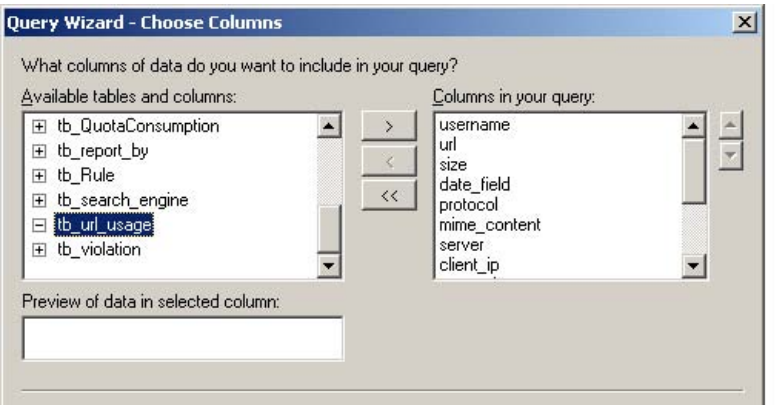


FIGURE 8-16. Query Wizard - Choose Columns screen.

5. Under **Query Wizard - Filter Data**, filter the data to specify which rows to include in your query.

   For example, select "username" in **Column to filter**, then choose "begins with" in the drop-down list under **Only include rows where > username**, and then select "username." Click **Next**.

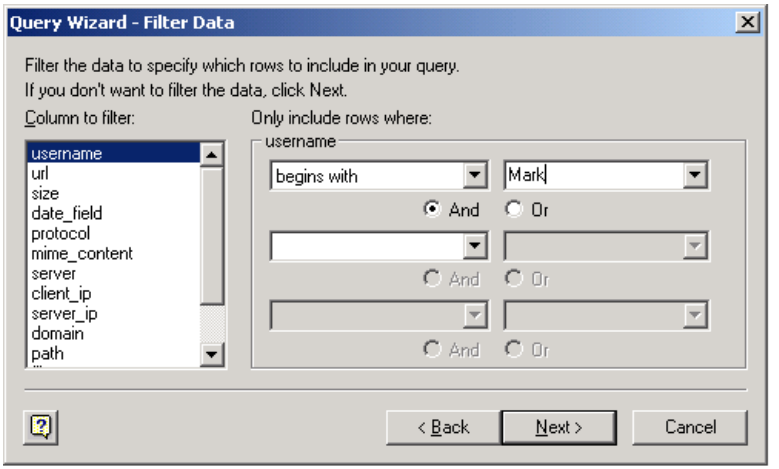


FIGURE 8-17. Query Wizard - Filter Data screen.

6. Under **Query Wizard - Sort Order**, specify the type under the **Sort by** field, and then specify how the data must be sorted:
   - Ascending or
   - Descending

   Click **Next**.
7. In the next screen, select **Return Data to Microsoft Excel**, and then click **Finish**. Select the location where to save the data (Existing worksheet, New worksheet, PivotTable report). Click **OK**.

TABLE 8-2. Major database tables for IWSS logging/reporting.

Table Name	Example Columns
tb_url_usage	username, url, size, date_field, protocol, mime_content, server, client_ip, server_ip, domain, path, file_name, operation, uid
tb_report_by	Period, category, entity_type, entity_name
tb_violation	username, date_field, protocol, url, malicious_entity, file_name, entity_name, action, scan_type, blocked_by, rule_name, opp_id, group_name, category, uid
tb_performance_value	Server, date_field, Metric_value, Metric_id
tb_entity	EntityID, EntityType, EntityName
tb_entitytype	EntityType, EntityTypeName, Note
tb_policy	PolicyID, PolicyName, PolicyType, IsEnable, IsDefault, CreationTime, LastModifiedTime, Note
tb_policytype	PolicyType, TypeName, TimeToLive, UpdateVersion, Note

Table Name	Example Columns
tb_prioritylist	EntityID, PolicyID, Priority
tb_quotaconsumption	EntityType, EntityName, Digest, Consumption, Timeframe, LastUpdateTime
tb_rule	RuleID, PolicyID, ActiveTime, RuleValue
tb_search_engine	id, url

Chapter 9

Trend Micro Control Manager

This chapter introduces IWSS management via Control Manager, an antivirus and content security management solution. Here you will find information about its purpose, capabilities, install agent, and architecture.

Topics included in this chapter are:

- Control Manager Overview
- Outbreak Prevention Services
- Important Terms
- Understanding the Management Architecture
- About Agents
- Opening the Management Console
- Updating the Outbreak Prevention Policy
- Status Monitoring
- Configuration Replication

Control Manager Overview

Control Manager is a software management solution that gives you the ability to control antivirus and content security programs from a central location — regardless of the program's physical location or platform. This application can simplify the administration of a corporate antivirus and content security policy.

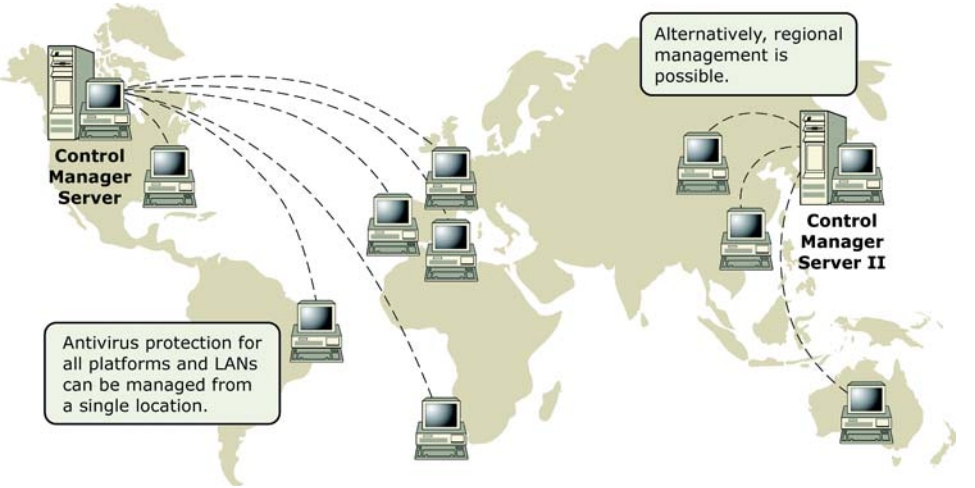


FIGURE 9-1. Control Manager managing a global antivirus and content security network.

Outbreak Prevention Services

Outbreak Prevention Services (OPS) are Trend Micro services available through Control Manager. OPS allows enterprises to take proactive steps against new virus threats before the necessary virus pattern files are available. By bridging the gap between threat notification and virus pattern delivery, enterprises can quickly contain virus outbreaks, minimize system damage, and prevent undue downtime.

OPS is a key component of the Trend Micro Enterprise Protection Strategy (EPS) – the culmination of a research initiative that identified best practices for preventing or deflecting potentially damaging virus attacks. This study was brought on by the apparent failure of conventional security measures to defend against new generation threats, such as CodeRed and Nimda.

What OPS provides

- Timely notification of new threats
- Continuous and comprehensive updates on the status of the outbreak
- Threat-specific recommendations on how to contain viruses
- Prompt delivery of virus-specific product settings, called “outbreak prevention policies"

Note: Additional information on the Enterprise Protection Strategy can be found on the Trend Micro Web site at http://www.trendmicro.com.

It was determined that enterprises – regardless of size – adhered to a remarkably similar set of staged procedures when responding to what Trend Micro now calls the “virus outbreak lifecycle.”

In response to these findings, Trend Micro created Outbreak Prevention Services to address concerns at each stage of the life cycle. OPS harnesses the three core strengths of Trend Micro:

- Enterprise-class antivirus and content security products
- TrendLabs— the Trend Micro ISO-certified virus research and technical support center
- Partnerships with best-of-breed network security vendors

and brings them together in a single powerful interface: Trend Micro Control Manager. With OPS, Control Manager provides answers to the following key security questions:

- Am I under attack?
- Can my system handle the attack?
- How should I respond to the attack?

Important Terms

The terms shown below are used throughout the chapter; thus, you need to become familiar with these terms.

Control Manager Server

The Control Manager server is the machine on which the Control Manager application is installed. The Control Manager Web-based management console, which controls the Control Manager system, runs on this server.

Agent

The agent is an application installed on a product-server that allows Control Manager to manage the product. It receives commands from the Control Manager server, and then applies them to the managed product. It also collects logs from the product, and sends them to Control Manager. The Control Manager agent does not communicate with the Control Manager server directly. Instead, it interfaces with a component called the Communicator.

Communicator

The Communicator is the communications backbone of the Control Manager system; it is part of the Trend Micro management infrastructure. Commands from the Control Manager server to the managed products, and status reports from the products to the Control Manager server, all pass through this component. Only one Communicator is installed on each product server; the Communicator then handles the needs of all the agents on the aforementioned server.

Entity

An entity is a representation of a managed product on the **Product Directory** link. You see these icons in the directory tree of the **Entity** section. The directory tree is a composition of all managed entities, residing on the Control Manager console.

Understanding the Management Architecture

Control Manager uses a three-tier management architecture:

- Enterprise Protection Management Tier
- Product-level Management Tier
- Protection Tier

All protection occurs at the first tier called the ***Protection Tier***. Client applications of client-server products such as OfficeScan Enterprise Edition, and the servers of stand-alone products such as InterScan VirusWall, InterScan Web Security Suite, and ScanMail for Microsoft Exchange reside in this tier.

The management servers of client server products such as OfficeScan Corporate Edition and ServerProtect populate the ***Product-level Management Tier***. These servers enforce virus policies, and deploy updates to their client products.

All these products can be brought under a single Control Manager server in the ***Enterprise Protection Management Tier***. Using the Control Manager Web-based management console, you can enforce a uniform security policy for all your antivirus and content security products.

About Agents

Control Manager controls the first two tiers of its network using a system of applications called agents. These agents receive command inputs from the management console, and then apply them to the managed products. Agents also obtain status information from the products and send them back to the Control Manager server. The latter function allows you to view the status of your entire network at a glance.

The Control Manager agent package is actually composed of two components: the agent itself, and the Communicator. The Communicator handles secure-communication between agents and the Control Manager server. Only one Communicator is installed on a machine; thus if multiple products co-exist on a server, the product agents share the Communicator.

Opening the Management Console

There are two ways to access the management console: directly on the Control Manager server, or remotely, using a browser.

To access the management console on the server:

1. At the server, click **Start** > **Programs** > **Trend Micro Control Manager** > **Trend Micro Control Manager Server**.
2. Type your user name and password in the fields provided.
3. Click **Sign in**.

To access the management console via a browser:

1. Type the following in the browser address field:

   ```
   http://{host name or IP}/ControlManager
   ```

   where host name is the name of the server on which Control Manager is installed. The **Logon** screen opens.
2. Type your user name and password in the fields provided.
3. Click **Sign in**.

To log off from the management console:

Click **Sign Out** at the upper right corner of the management console.

Updating the Outbreak Prevention Policy

You can find the policies currently on your Control Manager server on the main Outbreak Commander screen. You must update your policies if you receive a notification of an outbreak that does not have a corresponding policy on the table.

Note: After installing a Control Manager server, Trend Micro strongly advises you to perform an **Update Now** task to update your policies immediately. For subsequent updates, use the **Scheduled Update** function.

To apply an outbreak prevention policy to IWSS:

1. Access the management console via Control Manager or remotely using a browser.
2. Click **Outbreak Commander** on the menu.
3. Select a policy (for example, WORM_BAGLE.H).

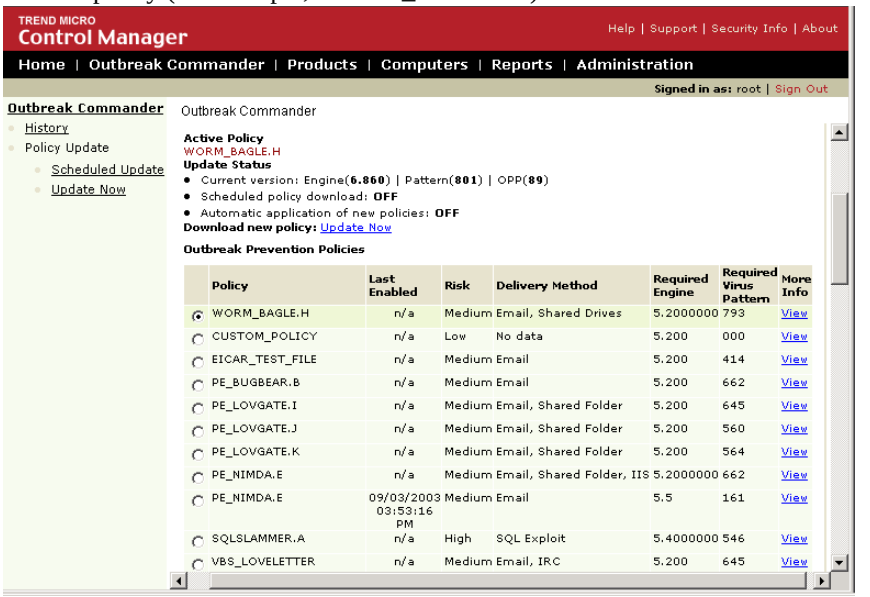


FIGURE 9-2. Outbreak Prevention Policy screen in the Control Manager Web console.

4. Click **Outbreak Prevention Wizard**.
5. In the next screen, click **Start**.
6. Under the **Prevention** tab, indicate the duration of the policy (in days) in the **Policy duration** field and indicate how the prevention stage must be applied in the **Deployment plan** field, which has three options:
   - **Deploy to All Entities Now (Default)**
   - **Deploy to All Immediately (Outbreak-Prevention)**
   - **Deploy to All Immediately (Outbreak-Scanning)**

7. Select **InterScan Web Security Suite for Solaris or Linux** and click **InterScan Web Security Suite for Solaris or Linux**. Indicate the entry points that must be blocked by this policy. Indicate the type of blocking to be implemented (Webmail site blocking, File name blocking, File name/true file type blocking, URL pattern blocking, and Web server blocking) and type the entries to be blocked in the text box provided.
8. Click **Next** to go to the **Notification** tab. On this screen, specify the recipient of the notification, method of notifying the recipients (email, pager), and the corresponding message to be sent.
9. Click **Next** to go to the **Scanning** tab (no configurations needed for IWSS). Click **Next** to go to the **Update** tab. Under the **Update** screen, specify how often you want to check for updates (interval of time and source; **Internet: Trend Micro update server** or **Other source**) and the method of deploying the updates (**Immediately to all destinations** or **According to a Deployment Plan**).
10. Click **Finish**.

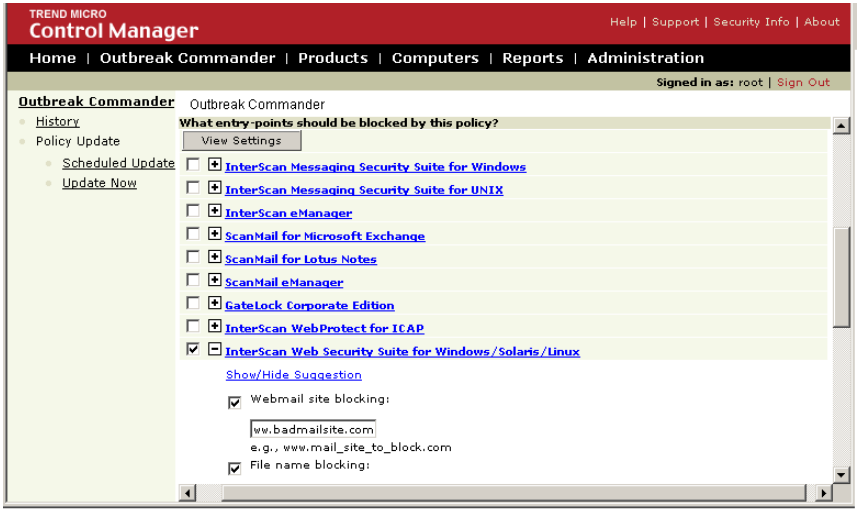


FIGURE 9-3. Use the settings recommended by Trend Micro, or modify them according to the needs of your network.

To view the status of IWSS:

1. Open the Control Manager management console.
2. Click **Products** on the menu.
3. In the left menu, select the target machine for the IWSS product (for this example, US-IWSS-115).

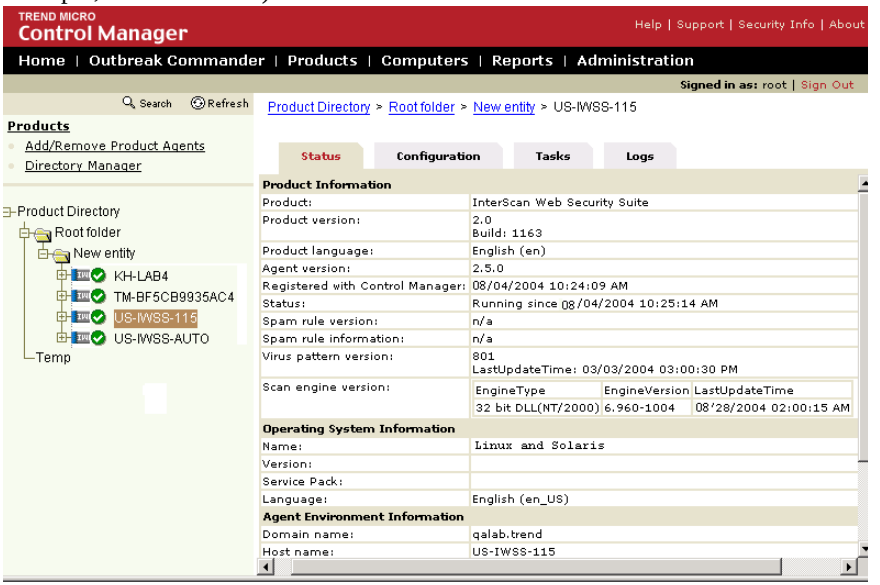


FIGURE 9-4. The Status screen provides product, operating system, and agent environment information.

To perform configuration replication for IWSS:

1. Open the Control Manager management console.
2. Click **Products**.
3. In the left menu, select the master IWSS machine (for this example, US-IWSS-115) that will perform the replication.

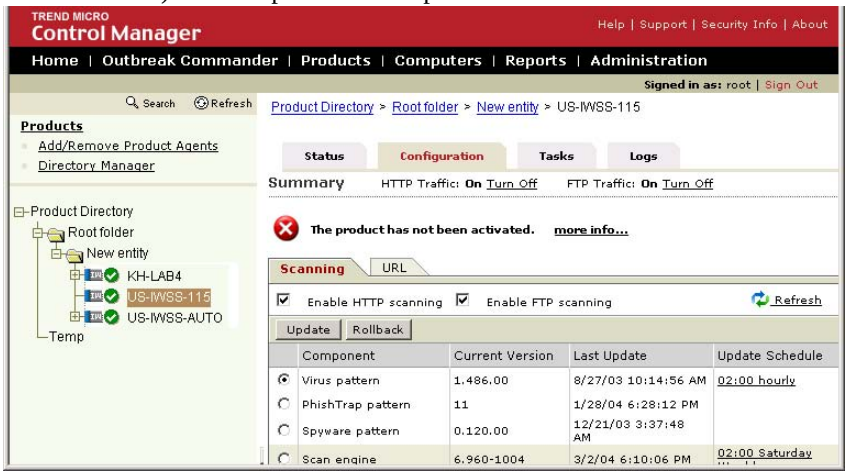


FIGURE 9-5. You can perform all the necessary configurations for IWSS within Control Manager.

4. The **Configuration** tab is used to configure the master IWSS machine. Select the product name in the drop-down menu under the **Select a product** field, and select the appropriate entry under the **Select a configuration** field. Click **Next**.

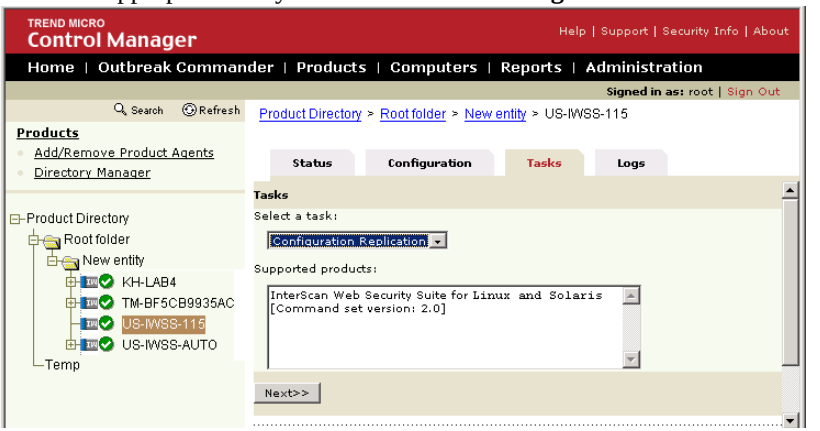


FIGURE 9-6. The selected IWSS servers for configuration replication have to be in the same service mode as the source IWSS server.

5. The IWSS console appears. Perform the desired configuration, and then click **Tasks**. Choose **Configuration Replication** in the drop-down menu of the **Select a task** field.

6. Click **Next**. In the next screen select an entity or folder for replication, and then click **Replication**.

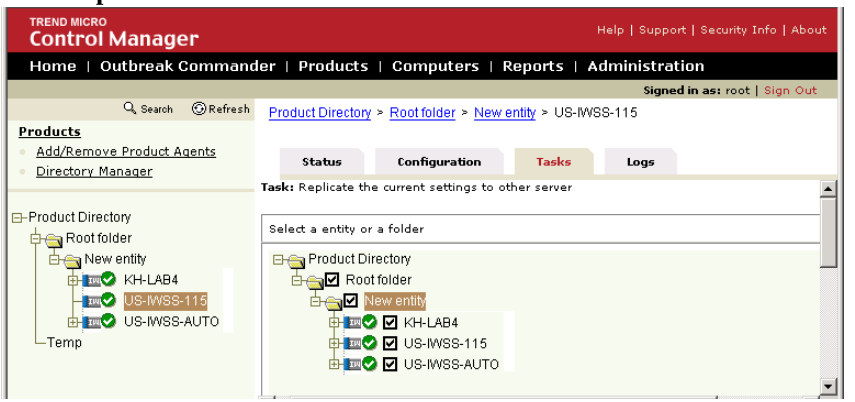


FIGURE 9-7. Select an entity or folder for configuration replication.

Chapter 10

Technical Support, Security Information, and Troubleshooting

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. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

If you need help or just have a question, please feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all of our registered users.

- To view a list of the worldwide support offices, go to:

  `http://kb.trendmicro.com`

- To view the latest Trend Micro product documentation, go to:

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

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 console and choosing **Support** from the drop-down in the 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
```

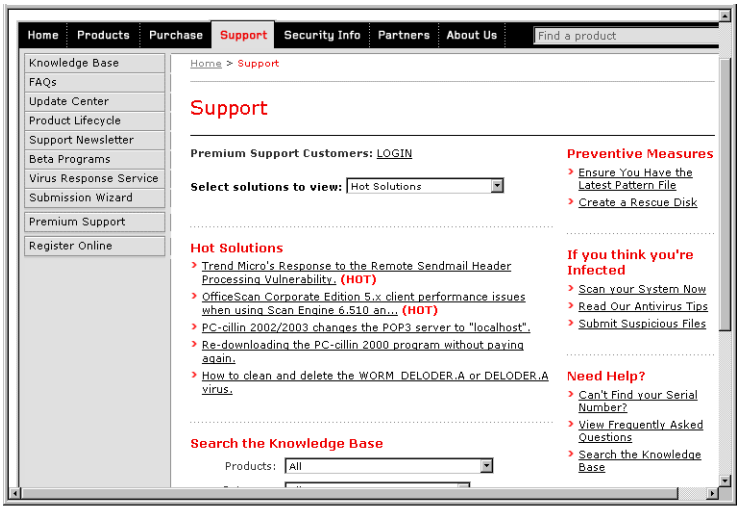


FIGURE 10-1. Trend Micro Technical Support site.

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 threats 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 reach the desktop.

To make this possible, TrendLabs, a global network of antivirus research and product support centers, provides continuous 24 x 7 coverage to Trend Micro customers around the world. TrendLabs' modern headquarters has earned ISO 9002 certification for its quality management procedures in 2000 - one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

Trend Micro is headquartered in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia–a global organization with more than 1,800 employees in 25 countries.

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

`http://www.trendmicro.com`

Contacting Trend Micro

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

`http://www.trendmicro.com/en/about/contact/overview.htm`

Note: The information on this Web site is subject to change without notice.

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.

Version Information

In addition to virus pattern file updates, Trend Micro also provides occasional scan engine and/or program upgrades. To find out exactly which virus pattern, PhishTrap, spyware, URL filtering database pattern numbers, or scan engine build you are running, click **Summary** in the left menu of the IWSS console.

About the Scan Engine Updates

By storing the most time-sensitive virus information in external data files such as the virus pattern file, the anti-spam database, and outbreak prevention policies, Trend Micro is able to minimize the number of scan engine upgrades while at the same time keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. New engines are released, for example, when:

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

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

`http://www.trendmicro.com`

FIGURE 10-2. Where to find the current version of the scan engine

Knowledge Base

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 the Readme document you received with your product. Readme files for Trend Micro products 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.

FIGURE 10-3. 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 threats 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 message, 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 threats expected to trigger in the current week, and describes the 10 most prevalent threats around the globe for the current week
- View a Virus Map of the top 10 threats around the globe
- Consult the Virus Encyclopedia, a compilation of known threats including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the threat, 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 threats
  - The Trend Micro *Safe Computing Guide*
  - A description of risk ratings to help you understand the damage potential for a threat rated Very Low or Low vs. Medium or High risk
  - A glossary of virus and other security threat 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 console.
2. Click **Security Info** from the drop-down menu at the top-right panel of the screen. The **Security Information** screen appears.

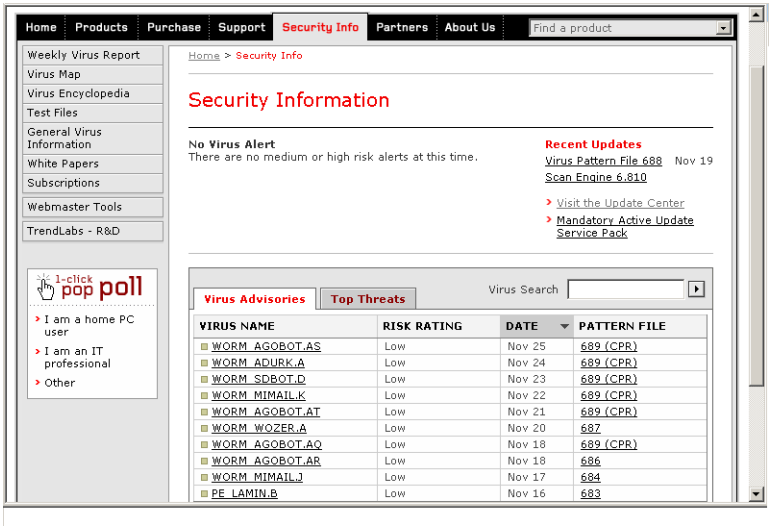


FIGURE 10-4. A multitude of virus and product information is available from the Security Information screen.

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 threats. 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.

Damage Cleanup Services

Trend Micro Damage Cleanup Services help restore your Windows system after a Trojan attack. A Trojan, like a virus, attacks your system (but unlike a virus, a Trojan cannot self-replicate).

When a Trojan is executed, you will likely experience unwanted system problems in operation, and sometimes loss of valuable data. These are indications that you should run Trend Micro Damage Cleanup Services on your system.

Two versions of Damage Cleanup Services are available at no charge–one for Trend Micro customers, and one for the general public. Download Damage Cleanup Services from the following Web site:

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

Both versions support the following:

- Terminates malware instances in memory
- Removes malware registry entries
- Removes malware entries from system files
- Scans for and deletes malware copies in local hard drives

Troubleshooting

How to turn on the verbose log

1. Set verbose=1 in the [http] section in the `intscan.ini` file
2. Restart the service.

IWSS cannot detect a virus

1. Open the IWSS console and click **Administration > Product License**.
2. Check if the product license status is activated.

URL filtering cannot block the URL specified in the policy

Option 1: Check the license status

1. Open the IWSS console and click **Administration > Product License**.
2. Check if the product license status is activated.

> **Note:** The Activation Codes for IWSS virus detection and URL filtering module are different.

Option 2: Check if the policy has been deployed

1. Open the IWSS console and click **HTTP > URL Filtering Policies > Policy List**.
2. Select a policy and click **Deploy Policies**.

> **Note:** The Global Policy is automatically deployed. User-configured policies are not automatically deployed

Option 3: Check the database connection

1. Open the IWSS console and click **HTTP > Configuration > Database**.
2. Click **Test Database Connection**.

A "cannot find server or DNS error" message appears after entering the user and password credentials when going through the proxy to a site with NTLM authentication.

To resolve this issue:

1. Open Internet Explorer and click **Tools > Internet Options** from the main menu.
2. Click the **Advanced** tab. Under the **HTTP 1.1 settings** section, select **Use HTTP 1.1** and **Use HTTP 1.1 through proxy connections**.
3. Click **OK**.

Some Internet applications do not function properly when scanned through ICAP (for example, certain types of custom Internet programs, stock tickers, download agents, real-time video, etc.).

To resolve this issue:

Add `client_skip_content` or `server_skip_content` in the [http] section of the `intscan.ini` file (see *Configuration Files* starting on page C-1 for more information). The `client_skip_content` or `server_skip_content` looks for a particular pattern in the HTTP header. If an entry in the HTTP header is an exact match with the `client_skip_content` or `server_skip_`content, the specified content works properly but will not be scanned (for example, `client_skip_content=User-Agent: Real-time Test Tool, server_skip_content=Host: www.yahoo.com`).

How to skip the progress-scanning feature

To skip the progress-scanning feature, add `skip_type_intermediate` under the [http] section of the `intscan.ini` file. The `skip_type_intermediate` takes the MIME-type content that you want to bypass (for example, `skip_type_intermediate = text/html, application/x-rma`).

Where are the memory block lists stored?

Infected URLs will be added to the list so that the next user will not have access to the same URL. Each entry in the memory block list is stored in `infectedB.ini` in `the /etc/iscan/` directory (by default). Manually stop the HTTP service to create and view this file.

What is the effect on performance if the URL access log is ON?

There will be a 10-20% performance degradation if the URL access log is turned ON (the default setting is OFF).

Appendix A

Glossary of Terms

This glossary describes special terms as used in this document or the online help.

Term	Explanation
action (*Also see* target and notification)	The operation to be performed when: - a virus has been detected - spam has been detected - a content violation has occurred - an attempt was made to access a blocked URL, or - file blocking has been triggered. Actions typically include clean and deliver, quarantine, delete, or deliver/transfer anyway. Delivering/transferring anyway is not recommended—delivering a virus-infected message or transferring a virus-infected file can compromise your network.
activate	To enable your IWSS software after completion of the registration process. IWSS will not be operable until product activation is complete. Activate during installation on the **Product Activation** screen, or after installation (in the management console) on the **Administration** > **Product License** screen.
Activation Code	A 37-character code, including hyphens, that is used to activate InterScan Web Security Suite. Here is an example of an Activation Code: AC-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 *Also see* Registration Key.

Term	Explanation
ActiveUpdate	ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files via the Internet or the Trend Micro Total Solution CD.
Active Directory	A directory service from Microsoft that is a part of Windows 2000.
ActiveX	A type of open software architecture that implements object linking and embedding, enabling some of the standard interfaces, such as downloading of Web pages.
ActiveX malicious code	An ActiveX control is a component object embedded in a Web page which runs automatically when the page is viewed. ActiveX controls allow Web developers to create interactive, dynamic Web pages with broad functionality such as HouseCall, Trend Micro's free online scanner. Hackers, virus writers, and others who want to cause mischief or worse may use ActiveX malicious code as a vehicle to attack the system. In many cases, the Web browser can be configured so that these ActiveX controls do not execute by changing the browser's security settings to "high."
address	Refers to a networking address (*see* IP address) or an email address, which is the string of characters that specify the source or destination of an email message.
administrator	Refers to “system administrator"—the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.
adware	Advertising-supported software in which advertising banners display while the program is running. Adware that installs a “backdoor”; tracking mechanism on the user's computer without the user's knowledge is called “spyware.”
alert	A message intended to inform a system's users or administrators about a change in the operating conditions of that system or about some kind of error condition.

Term	Explanation
anti-relay	Mechanisms to prevent hosts from “piggybacking” through another host’s network.
antivirus	Computer programs designed to detect and clean computer viruses.
approved sender	A sender whose messages are always allowed into your network.
archive	A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.
attachment	A file attached to (sent with) an email message.
audio/video file	A file containing sounds, such as music, or video footage.
binary	A number representation consisting of zeros and ones used by practically all computers because of its ease of implementation using digital electronics and Boolean algebra.
block	To prevent entry into your network.
blocked sender	A sender whose messages are never allowed to enter your network.
boot sector	A sector is a designated portion of a disk (the physical device on which data is written and read). The boot sector contains the data used by your computer to load and initialize the computer’s operating system.
boot sector virus	A boot sector virus is a virus targeted at the boot sector (the operating system) of a computer. Computer systems are most likely to be attacked by boot sector viruses when you boot the system with an infected disk from the floppy drive - the boot attempt does not have to be successful for the virus to infect the hard drive. Also, there are a few viruses that can infect the boot sector from executable programs. These are known as multi-partite viruses and they are relatively rare. Once the system is infected, the boot sector virus will attempt to infect every disk that is accessed by that computer. In general, boot sector viruses can be successfully removed.

Term	Explanation
browser	A program which allows a person to read hypertext, such as Internet Explorer. The browser gives some means of viewing the contents of nodes (or "pages") and of navigating from one node to another. A browser acts as a client to a remote Web server.
cache	A small fast memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc.
case-matching	Scanning for text that matches both words and case. For example, if "dog" is added to the content-filter, with case-matching enabled, messages containing "Dog" will pass through the filter; messages containing "dog" will not.
cause	The reason a protective action, such as URL-blocking or file-blocking, was triggered—this information appears in log files.
checksumming	The process of calculating a computed value which depends on the contents of a block of data, and which is transmitted or stored along with the data to detect corruption of the data.
clean	To remove virus code from a file or message.
CLI	command line interface, a user interface common to MS-DOS computers. The user sees the command line on the monitor and a prompt that is waiting to accept instructions from the user. The user types in the command, the computer acts on that command and then issues a new prompt for the next instruction from the user. CLI operating systems are becoming less used as GUI operating systems gain in popularity. In a GUI operating system, such as Windows, the user responds to graphic images on the screen instead of typing in commands in response to a prompt.
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.
client-server environment	A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to some protocol, asking for information or action, and the server responds.

Term	Explanation
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
configuration	Selecting options for how IWSS will function, for example, selecting whether to quarantine or delete a virus-infected email message.
content violation	An event that has triggered the content filtering policy.
daemon	A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.
damage routine	The destructive portion of virus code, also called the payload.
default	A value that pre-populates a field in the management console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.
directory	A node, which is part of the structure in a hierarchical computer file system. A directory typically contains other nodes, folders, or files.
directory path	The subsequent layers within a directory where a file can be found.
disclaimer	A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message.
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.

Term	Explanation
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution," uses the Domain Name System (DNS).
DoS (Denial of Service) attack	Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.
download (noun)	Data that has been downloaded, for example, from a Web site via HTTP.
download (verb)	To transfer data or code from one computer to another. Downloading often refers to transfer from a larger "host" system (especially a server or mainframe) to a smaller "client" system.
executable file	A binary file containing a program in machine language which is ready to be executed (run).
FAQ	Frequently Asked Questions—A list of questions and answers about a specific topic.
file	An element of data, such as an email message or HTTP download.
file-infecting virus	File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. A minority of these viruses are very destructive and attempt to format the hard drive at a pre-determined time or perform some other malicious action. In many cases, a file-infecting virus can be successfully removed from the infected file. However, if the virus has overwritten part of the program's code, the original file will be unrecoverable
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.

Term	Explanation
file name extension	The portion of a file name (such as .dll or .xml) which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.
firewall	A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.
FTP	A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.
gateway	An interface between an information source and a Web server.
grayware	A category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.
GUI	Graphical User Interface—The use of pictures rather than just words to represent the input and output of a program. This contrasts with a command line interface where communication is by exchange of strings of text.
hard disk (or hard drive)	One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks.
heuristic rule-based scanning	Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.
HTTP	Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
host	A computer connected to a network.

Term	Explanation
HouseCall	A free virus scanning and cleaning product from Trend Micro. HouseCall can detect and clean viruses found on your hard drive, but HouseCall does not provide real-time protection. In other words, HouseCall can help you to discover and clean up an existing problem, but will not prevent future ones, nor will HouseCall protect against worms, or mass-mailing programs.
ICSA	ICSA Labs is an independent division of TruSecure Corporation. For over a decade, ICSA has been the security industry's central authority for research, intelligence, and certification testing of products. ICSA Labs sets standards for information security products and certifies over 90% of the installed base of antivirus, firewall, IPSec, cryptography, and PC firewall products in the world today.
image file	A file containing data representing a two-dimensional scene, in other words, a picture. Images are taken from the real world, for example, via a digital camera, or they may be generated by computer using graphics software.
installation wizard	The setup program used to install IWSS.
integrity checking	*See* checksumming.
IntelliScan	IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true file type recognition, and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by a harmless extension name.
Internet	A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.
interrupt	An asynchronous event that suspends normal processing and temporarily diverts the flow of control through an "interrupt handler" routine.
“in the wild”	Describes known viruses that are actively circulating. *Also see* “in the zoo.”
“in the zoo”	Describes known viruses that are currently controlled by antivirus products. *Also see* “in the wild.”

Term	Explanation
intranet	Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.
IP	Internet Protocol—*See* IP address.
IP address	Internet address for a device on a network, typically expressed using dot notation such as 123.123.123.123.
IT	Information technology, to include hardware, software, networking, telecommunications, and user support.
Java file	Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet's code is transferred to your system and is executed by the browser's Java Virtual Machine.)
Kerberos authentication	An authentication system developed at the Massachusetts Institute of Technology (MIT). Kerberos is designed to enable two parties to exchange private information across an otherwise open network. It works by assigning a unique key, called a ticket, to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message.
KB	Kilobyte—1024 bytes of memory.
LDAP	Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it's a simpler version of X.500, LDAP is sometimes called X.500-lite. Although not yet widely implemented, LDAP should eventually make it possible for almost any application running on virtually any computer platform to obtain directory information, such as email addresses and public keys. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

Term	Explanation
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building.
license	Authorization by law to use IWSS.
license certificate	A document that proves you are an authorized user of IWSS.
link (also called hyperlink)	A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.
listening port	A port utilized for client connection requests for data exchange.
load balancing	Distributing processing and communications activity evenly across a computer network so that no single device is overwhelmed. Load balancing is especially important for networks where it's difficult to predict the number of requests that will be issued to a server. Busy Web sites typically employ two or more Web servers in a load balancing scheme. If one server starts to get swamped, requests are forwarded to another server with more capacity. Load balancing can also refer to the communications channels themselves.
logic bomb	Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met.
MAC address	Media Access Control address, a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sublayers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network medium. Consequently, each different type of network medium requires a different MAC layer.

Term	Explanation
MacroTrap	A Trend Micro utility that performs a rule-based examination of all macro code that is saved in association with a document. macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).
macro virus	Unlike other virus types, macro viruses aren't specific to an operating system and can spread via email attachments, Web downloads, file transfers, and cooperative applications.
management console	The IWSS user interface.
mass mailer (also known as a Worm)	A malicious program that has high damage potential, because it causes large amounts of network traffic.
match case	*See* case-matching.
MB	Megabyte—1024 kilobytes of data.
message	An email message, which includes the message subject in the message header and the message body.
message body	The content of an email message.
Microsoft Office file	Files created with Microsoft Office tools such as Excel or Microsoft Word.
mixed threat attack	Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.
multi-partite virus	A virus that has characteristics of both boot sector viruses and file-infecting viruses.
notification (*Also see* action and target)	A message that is forwarded to one or more of the following: - system administrator - sender of a message - recipient of a message, file download, or file transfer The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download.

Term	Explanation
offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
online help	Documentation that is bundled with the GUI.
operating system	The software which handles tasks such as the interface to peripheral hardware, scheduling tasks, and allocating storage. In this documentation, the term also refers to the software that presents a window system and graphical user interface.
parameter	A variable, such as a range of values (a number from 1 to 10).
partition	A logical portion of a disk. (*Also see* sector, which is a physical portion of a disk.)
pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
payload	Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.
PC	Personal Computer—A general-purpose single-user microcomputer designed to be operated by one person at a time.
phish	Phishing is a rapidly growing form of fraud that seeks to fool Web users into divulging private information by mimicking a legitimate Web site. In a typical scenario, an unsuspecting user gets an urgent (and authentic-looking) email message, telling him or her there is a problem with their account that they must fix immediately or the account will be closed. The message typically includes the URL of a Web site that looks exactly like the Web site of the user's bank or credit card company. The user is urged to log on to the bogus site and confirm his or her account information. Any data entered at the site, however, is redirected to a malicious hacker who steals the user name, password, credit card number, Social Security number, or whatever data that the victim entered.
polymorphic virus	A virus that is capable of taking different forms.

Term	Explanation
port	A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it.
proxy	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
purge	To delete all, as in getting rid of old entries in the logs.
quarantine	To place infected email messages, email messages with infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your IWSS server.
queue	A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.
recipient	The person or entity to whom an email message is addressed.
registration	The process of identifying yourself as a Trend Micro customer, using a product Registration Key, on the Trend Micro Online Registration screen. *https://olr.trendmicro.com/registration*
Registration Key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: RK-27RT-UY4Z-39HB-MNW8 *Also see* Activation Code
relay	To convey by means of passing through various other points.
removable drive	A removable hardware component or peripheral device of a computer, such as a zip drive.
replicate	To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.

Term	Explanation
scan	To examine items in a file in sequence to find those that meet a particular criteria.
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
sector	A physical portion of a disk. (*Also see* partition, which is a logical portion of a disk.)
seat	A license for one person to use InterScan VirusWall for SMB.
Secure Password Authentication	An authentication process, by which communications can be protected, using for example, encryption and challenge/response mechanisms.
sender	The person who is sending an email message to another person or entity.
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers.
server farm	Also referred to as server cluster, computer farm or ranch. A server farm is a group of network servers that are housed in one location. A server farm streamlines internal processes by distributing the workload between the individual components of the farm and expedites computing processes by harnessing the power of multiple servers. The farms rely on load-balancing software that accomplishes such tasks as tracking demand for processing power from different machines, prioritizing the tasks and scheduling and rescheduling them depending on priority and demand that users put on the network. When one server in the farm fails, another can step in as a backup.
shared drive	A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses.
SOCKS4	A protocol that relays TCP (transmission control protocol) sessions at a firewall host to allow application users transparent access across the firewall.

Term	Explanation
spyware	Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used.
status bar	A feature of the user interface, that displays the status or progress of a particular activity, such as loading of files on your machine.
target (*Also see* action and notification)	The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.
Telnet	The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.
top-level domain	The last and most significant component of an Internet fully qualified domain name, the part after the last ".". For example, host *wombat.doc.ic.ac.uk* is in top-level domain "uk" (for United Kingdom).
Total Solution CD	A CD containing the latest product versions and all the patches that have been applied during the previous quarter. The Total Solution CD is available to all Trend Micro Premium Support customers.
traffic	Data flowing between the Internet and your network, both incoming and outgoing.
trigger	An event that causes an action to take place. For example, IWSS detects a virus in an email message. This *triggers* the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.
Trojan Horse	A malicious program that is disguised as something benign.
true file type	Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).

Term	Explanation
TTL	Time to Live, a field in the Internet Protocol (IP) that specifies how many more hops a packet can travel before being discarded or returned.
URL	Universal Resource Locator—A standard way of specifying the location of an object, typically a Web page, on the Internet, for example, *www.trendmicro.com*. The URL maps to an IP address using DNS.
virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
virus kit	A template of source code for building and executing a virus, available from the Internet.
virus trap	Software that helps you capture a sample of virus code for analysis.
virus writer	Another name for a computer hacker, someone who writes virus code.
Web	The World Wide Web, also called the Web or the Internet.
Web server	A server process running at a Web site which sends out Web pages in response to HTTP requests from remote browsers.
wildcard	For example, an asterisk (*) represents any characters. In the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a "wildcard," can be used for any number or suit in the card deck.
working directory	The destination directory in which the main application files are stored, such as C:\Program Files\Trend Micro\IWSS.

Appendix B

Mapping File Types to Block with MIME Content-types

The following table describes file types that you can enter in the **Other file types** fields (**HTTP > Scanning > Virus Scan Rule** or **FTP** > **Scanning > Target**) when blocking corresponding MIME content-types. For example, if you type `afc`, both the `audio/aiff` and `audio/x-aiff` MIME content-types will be blocked.

Table 1: Mapping of other file types with MIME content-types.

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

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

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

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

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

Appendix C

Configuration Files

There are three types of configuration files (main, protocol module, scanning module). All the configuration files are in the `{IWSS root}` directory; the default location for `{IWSS root} is C:\Program Files\Trend Micro\IWSS`. The main configuration file is in `intscan.ini`.

- Settings specific to virus scanning are in:
  `{IWSS root}\HTTP\IWSSPIScanVsapi.dsc`
- Settings that are specific to the ICAP protocol are in:
  `{IWSS root}\HTTP\IWSSPIProtocolIcap.pni`
- Settings that are specific to the stand-alone proxy are in:
  `{IWSS root}\HTTP\IWSSPIProtocolHttpProxy.pni`
- Settings for URL filtering scanning module are in:
  `{IWSS root}\HTTP\IWSSPIUrlFilter.dsc`
- Settings specific to reporting are in:
  `{IWSS root}\report.ini`
- Settings for the URL Categorization database are in:
  `{IWSS root}\HTTP\urlfcIFX.ini`
- Settings for default URL categories and their mapping information are in:
  `{IWSS root}\HTTP\urlfcMapping.ini`
- Settings for the list of IP address and IP ranges of all machines allowed to access the IWSS server for the purpose of proxying the HTTP requests are in:
  `{IWSS root}\HTTP\ClientACL.ini`

- Settings for rules that define what ports IWSS will forward HTTP requests to are in:
  `{IWSS root}\HTTP\HttpPortPermission.ini` (
- Settings for rules that define what ports IWSS will allow HTTPS tunneling to are in:
  `{IWSS root}\HTTP\HttpsConnectACL.ini`
- Settings for list of IP address and IP ranges of trusted servers are in:
  `{IWSS root}\HTTP\ServerIPWhiteList.ini`

The IWSS console varies depending on which modules are installed. If you have been using a previous version of IWSS, there are also many new features available in IWSS that require new `.ini` file entries.

Protocol Handlers

Functions responsible for interpreting and processing messages in some recognized transmission protocols are encapsulated in a dynamic library referred to as a protocol handler. IWSS provides a choice of either an ICAP protocol handler, which enables IWSS to act as an ICAP server, or an HTTP proxy handler, wherein IWSS acts like a direct HTTP proxy server. The application binary is independent of the protocol handler, allowing the same application to support different protocols with a configuration change.

Provide the complete path of the active configuration file of the protocol in the `main/protocol_config_path` entry in the `intscan.ini` file application.

Protocol handlers require their own specific configuration files, which contain entries that pertain only to that protocol. These protocol configuration files are denoted with a ".pni" filename extension.

Scanning Modules

Traffic scanning functionality is provided through dynamic libraries known as scanning modules. The first scanning module available to IWSS provides content scanning using the scan engine.

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

Appendix D

Platforms, Compression, and Encoding

Trend Micro has developed scan engines for all major platforms, including Windows, Unix, and DOS (individual platforms are listed below). In addition, the scan engines recognize all file types, more than 20 compression types, major encoding algorithms, Microsoft Office macros, and Web scripting languages. No known viruses or network exploits get past the engine, and there are multiple layers of analysis and protection that guard against unknown threats.

Password Protected/Encrypted Files

Since files must be opened to be scanned, password-protected or encrypted files cannot be scanned. These files are recognized as unable to be opened (and therefore un-scannable). The administrator can designate the entire class for automatic quarantine, or choose to have the scan engine ignore these files.

Platforms

- Windows, including Windows 2003, 2000, NT 4.x, NT 3.5x, XP, Me, 98, and 95
- Unix, including Solaris, all major flavors of Linux, IBM AS/400, OS/390
- DOS

Encoding

- MIME
- UUencode
- Bin/Hex

File types

- Executables, including .exe, .com, .lnk, .bas, .reg
- Library files, including .dll
- Others, including .hlp and.chm
- Microsoft Office files (see *Macro Scripts*, below)

Compression

- Zip
- Arj
- Cab

Macro Scripts

- Word Basic
- VBA (Visual Basic for Applications)
- VBA3

Note: Examples of applications that host Macro scripts are Microsoft Word, Excel, and PowerPoint.

Scripting Languages

- JavaScript
- VBScript

Appendix E

Virus Action and Scan-behind

Cleanable Files

	First access to the URL			Subsequent access to the URL	
Scan Action	**File Size**	**Actions to the file downloaded**	**Action observed**	**Actions to the file downloaded**	**Action observed**
Clean	**<X**	Clean and pass	Download the file without noticing that the file is infected and had been cleaned	Clean and pass	Download the cleaned file
Delete	**<X**	Delete	Show a warning message that the infected file is deleted	Block the URL	Show a warning message that the URL is blocked
Quarantine	**<X**	Move the infected file to the quarantine directory	Show a warning message that the infected file is quarantined	Block the URL	Show a warning message that the URL is blocked

where **X** is the size of file that triggers “scan-behind”

Cleanable Files

	First access to the URL			Subsequent access to the URL	
Scan Action	**File Size**	**Actions to the file downloaded**	**Action observed**	**Actions to the file downloaded**	**Action observed**
Clean	**>=X**	Pass the file but do scan-behind	Download the infected file	Clean and pass	Download the cleaned file
Delete	**>=X**	Pass the infected file, but do scan-behind and delete the infected file from the IWSS server	Download the infected file	Block the URL	Show a warning message that the URL is blocked
Quarantine	**>=X**	Move the infected file to the quarantine directory	Download the infected file	Block the URL	Show a warning message that the URL is blocked

where **X** is the size of file that triggers “scan-behind”

Non-cleanable Files

	First access to the URL			Subsequent access to the URL	
Scan Action	**File Size**	**Actions to the file downloaded**	**Action observed**	**Actions to the file downloaded**	**Action observed**
Pass	**<X**	Pass the file	Download the file without noticing that the file is infected	Pass the file	Download the file without noticing that the file is infected
Delete	**<X**	Delete	Show a warning message that the infected file is deleted	Block the URL	Show a warning message that the URL is blocked
Quarantine	**<X**	Move the infected file to the quarantine directory	Show a warning message that the infected file is quarantined	Block the URL	Show a warning message that the URL is blocked

where **X** is the size of file that triggers “scan-behind”

Non-cleanable Files

	First access to the URL			Subsequent access to the URL	
Scan Action	**File Size**	**Actions to the file downloaded**	**Action observed**	**Actions to the file downloaded**	**Action observed**
Pass	**>=X**	Pass the file	Download the file without noticing that the file is infected	Pass the file	Download the file without noticing that the file is infected
Delete	**>=X**	Pass the file	Download the file without noticing that the file is infected	Block the URL	Show a warning message that the URL is blocked
Quarantine	**>=X**	Pass the file	Download the file without noticing that the file is infected	Block the URL	Show a warning message that the URL is blocked

where **X** is the size of file that triggers “scan-behind”

Password-protected Compressed Files

	First access to the URL			Subsequent access to the URL	
Scan Action	**File Size**	**Actions to the file downloaded**	**Action observed**	**Actions to the file downloaded**	**Action observed**
Pass	**<X**	Pass the file	Download the file	Pass the file	Download the file
Delete	**<X**	Delete	Show a warning message that it is a password-protected file and is deleted	Delete	Show a warning message that it is a password-protected file and is deleted
Quarantine	**<X**	Move the password-protected file to the quarantine directory	Show a warning message that the password-protected file is quarantined	Move the password-protected file to the quarantine directory	Show a warning message that the password-protected file is quarantined

where **X** is the size of file that triggers “scan-behind”

Password-protected Compressed Files

	First access to the URL			Subsequent access to the URL	
Scan Action	**File Size**	**Actions to the file downloaded**	**Action observed**	**Actions to the file downloaded**	**Action observed**
Pass	**>=X**	Pass the file	Download the file	Pass the file	Download the file
Delete	**>=X**	Put the URL into the allow list, and then delete the password-protected file	Download the file	Check the URL if it match. It will not download the URL if the URL match.	Show a warning message that it is a password-protected file and is deleted
Quarantine	**>=X**	Move the password-protected file to the quarantine directory	Download the file	Move the password-protected file to the quarantine directory	Show a warning message that the password-protected file is quarantined

where **X** is the size of file that triggers “scan-behind”

Macros

	First access to the URL			Subsequent access to the URL	
Scan Action	**File Size**	**Actions to the file downloaded**	**Action observed**	**Actions to the file downloaded**	**Action observed**
Pass	**<X**	Pass the file	Download the file	Pass the file	Download the file
Clean	**<X**	Clean the macro	Download the file with the macro cleaned	Clean the macro	Download the file with the macro stripped off
Quar-antine	**<X**	Move the macro file to the quarantine direc-tory	Show a warning message that the macro file is quar-antined	Block the URL	Show a warn-ing message that the URL is blocked

where **X** is the size of file that triggers “scan-behind”

Macros

	First access to the URL			Subsequent access to the URL	
Scan Action	**File Size**	**Actions to the file downloaded**	**Action observed**	**Actions to the file downloaded**	**Action observed**
Pass	**>=X**	Pass the file	Download the file	Pass the file	Download the file
Clean	**>=X**	Pass the file, but perform scan-behind	Download the file	Clean the macro	Download the file with the macro stripped off
Quarantine	**>=X**	Move the macro file to the quarantine directory	Download the file	Block the URL	Show a warning message that the URL is blocked

where **X** is the size of file that triggers “scan-behind”

Index

Q

R

S

T

U

V

W

Trend Micro Incorporated
10101 N. De Anza Blvd.
Cupertino, CA., 95014 USA
www.trendmicro.com

For Sales:
Tel: +1-408-257-1500 (outside US and Canada)
Fax: +1-408-257-2003

Item Code: IHEM22346/50718