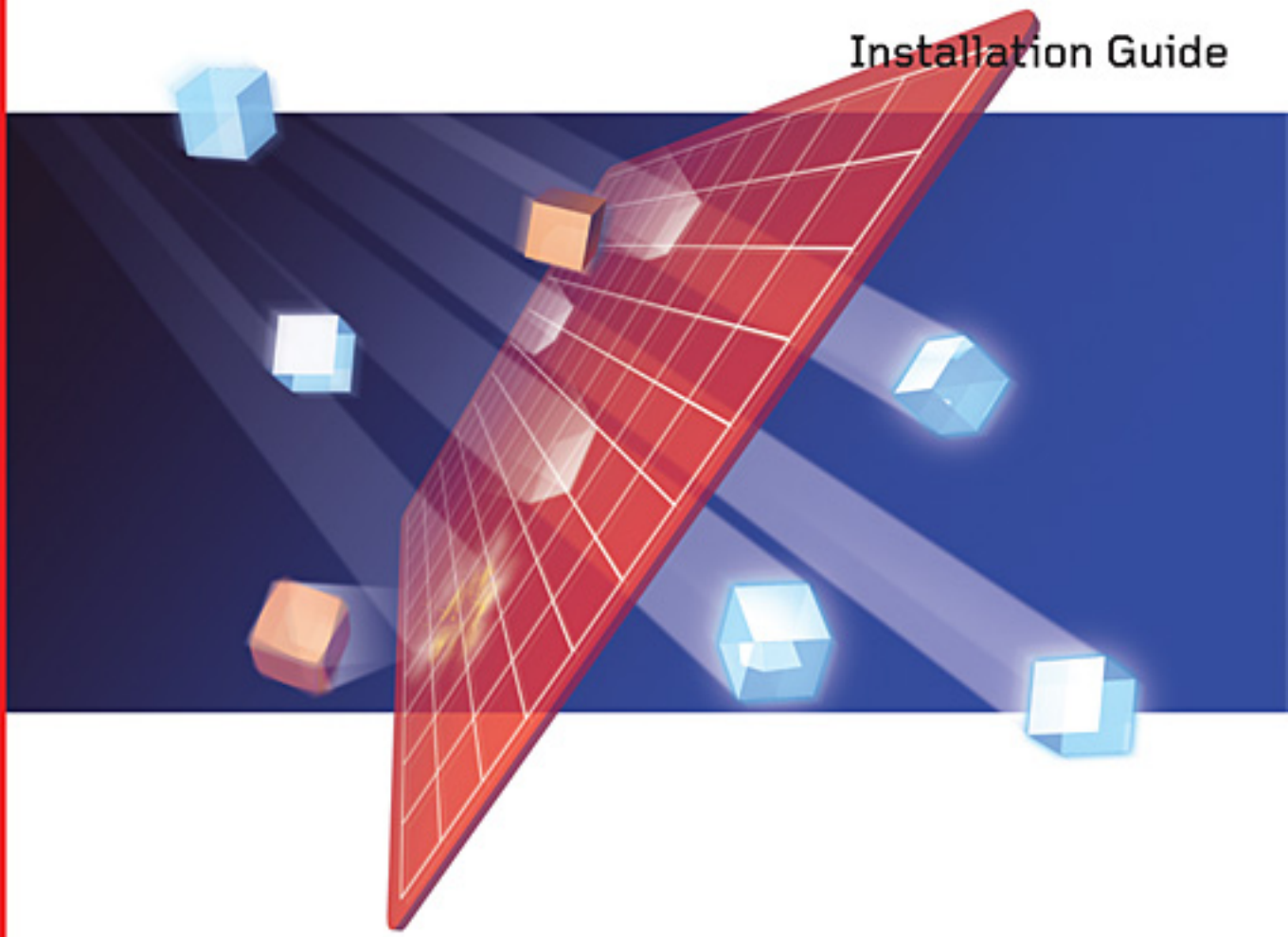
TREND MICRO™
InterScan™ Web Security Suite 2

Antivirus and Content Security at the Web Gateway

for Windows™

Installation Guide



TREND MICRO™

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

http://www.trendmicro.com/download

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

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.
Copyright 1997 Moscow Center for SPARC Technology. 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. Moscow Center for SPARC Technology 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

Copyright and Permission Notice

JFreeChart

PostgreSQL

MIT Kerberos Library
Copyright © 1985-2002 by the Massachusetts Institute of Technology. Export of software employing encryption from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting. WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original MIT software. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided “as is” without express or implied warranty.

Bouncy Castle Crypto APIs
Copyright (c) 2000 The Legion Of The Bouncy Castle
(http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Net-SNMP
Copyright 1989, 1991, 1992 by Carnage Mellon University

Derivative Work - 1996, 1998-2000, Copyright 1996, 1998-2000 The Regents of the University of California, All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission

notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of the Networks Associates Technology, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2003-2004, Sparta, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of Sparta, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT

OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Xerces-C XML Parser
Copyright 2005 Trend Micro, Inc.

Licensed under the Apache License, Version 2.0 (the “License”); you may not use this file except in compliance with the license. You may obtain a copy of the License at:

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Document Part No. IHEM22240/50407

Release Date: June 2005

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

The Installation Guide for Trend Micro™ InterScan™ Web Security Suite is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

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

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

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

Table of Contents

Chapter 3: Post-Installation Configuration

Chapter A: Technical Support and Troubleshooting

Chapter 1

Preparing to Install IWSS

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

Topics in this chapter include:

- Introducing IWSS and its main program components
- Listing new and significant features
- Introducing the IWSS documentation set
- Planning your installation, including such considerations as system requirements, the type of HTTP handler (Proxy Scan or ICAP), and type of FTP service
- Deciding on the type of HTTP proxy configuration (forward or reverse proxy) and transparency options that avoid the need to change client browser settings
- Introducing report and database setup
- Choosing a user identification method
- Migrating previous version settings

IWSS Overview

To help stop security risks from entering your network through the HTTP or FTP gateway, IWSS processes client requests and performs scanning and filtering tasks according to the program's configuration. Based on the policy configuration for the client making the request, IWSS performs the following operations:

- Scanning files in HTTP and FTP traffic for viruses, spyware/grayware and other security risks by comparing the file's binary patterns against signatures in the virus pattern file.
- Blocking Web pages with prohibited content, based on the site's classification in the URL filtering database.
- Verifying the digital signatures of Java applets and ActiveX objects.
- Instrumenting Java applets to enable real-time monitoring when applets run to inform clients of prohibited operations.
- Rejecting requests for URLs on the URL blocking list or in the Phish pattern file, or accepting requests for trusted URLs without further processing.
- Checking that the client has not exceeded their access quota, and rejecting the request when clients exceed the access quota for the time period.

To keep administrators informed about their gateway security, IWSS includes a Summary page about the program and pattern file versions in use, the most frequently blocked URLs, and recent spyware detections and other security events. For more detailed information about security and program events, IWSS is pre-configured with several reports to provide information about blocking events, traffic flow, spyware/grayware and cleanups. Additionally, files can be queried to provide the specific information required.

For an introduction to the main IWSS modules, see *Installation Planning* starting on page 6.

How IWSS Works

The core IWSS scanning and filtering functions are divided into three major components—the main service, the protocol handler, and the scan context.

- Main service: The main service accepts new HTTP and FTP connections and determines when the requested traffic is ready for the protocol handler.

- Protocol handler: The protocol handler reads and writes traffic on active sockets. When data accumulates from a request, the protocol handler invokes scanning and determines appropriate responses based on the scan result.
- Scan modules: In the IWSS architecture, scan modules provide the scanning and filtering functions such as virus scanning, URL blocking, signature verification, and so on. Based on scanning results, a transaction is accepted or rejected. Scanning includes three phases:
  - Pre-scanning: After file or page header data for a transaction is received, the scan module performs header-based rules such as URL categorization or enforcing restrictions based on the content-type.
  - Scanning: After pre-scanning completes, the file or page is processed according to the policy's configuration.
  - Post-scan: After all requested data is received or all scanning events are complete, status information about the scanning tasks are reported to the main program and written to the log files.

Using the Product Documentation

The documentation set for this product includes the following:

- Installation Guide—this Guide helps you get "up and running" by introducing IWSS, assisting with installation planning, implementation, and configuration, and describing the main post-installation configuration tasks. It also includes instructions on testing your installation using a harmless test virus, troubleshooting, and accessing Support.
- Administrator's Guide—this Guide provides detailed information about all IWSS configuration options. Topics include how to update your software to keep protection current against the latest risks, how to configure and use policies to support your security objectives, and using logs and reports.
- Readme file—the Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues, and release history.

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

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

- Online help—the purpose of online help is to provide “how to’s” for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online help is accessible from the IWSS management console.
- 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`

Minimum System Requirements

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

- Windows™ 2000 Server/Advanced Server with service pack 4 or Windows Server 2003 Standard Edition/Enterprise Edition with service pack 1
- PC with an Intel Pentium™ 4 2.4GHz processor or equivalent
- 1GB RAM; 2GB RAM recommended with URL filtering installed; an extra 128MB RAM if Applets and ActiveX security is installed.
- 2GB disk space for program files with URL filtering installed or 150MB disk space for program files without URL filtering (100 to 500MB free disk space for swap files)
- 125MB disk space to install MSDE (installed by default on a C: drive)
- A monitor with 800x600 or greater resolution
- Microsoft™ SQL Server 2000 (if not using MSDE 8.00.761, which is installed with IWSS)
- Microsoft™ Internet Explorer 6.0 to access the IWSS Web console or Netscape™ Navigator 7.0
- If using WCCP transparency, Trend Micro recommends using Cisco IOS versions:
  - 12.2(0) to 12.2(22). Avoid using versions 12.2(23).
  - 12.3(10) and above. Avoid using IOS versions from 12.3(0) to 12.3(9).

Directory Servers

To configure policies based on LDAP users and groups, IWSS can integrate with the following LDAP directories:

- Microsoft Active Directory 2000 and 2003
- Linux OpenLDAP Directory 2.2.16
- Sun™ Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)

ICAP Mode

- ICAP 1.0-compliant cache server (not required for stand-alone mode)
  - NetApp™ NetCache™ release 6.0.1, or
  - BlueCoat Systems™ SGOS 3.1.3.7, or
  - Cisco™ CE version 5.1.3, b15

Damage Cleanup Services (DCS) and Control Manager Support

- Supports DCS 3.0 for malicious code cleanup
- Supports TMCM 3.0 for consolidated management and reporting

Installation Notes

- Insufficient disk space and memory may cause performance issues and/or errors.
- For multiple IWSS ICAP servers to work properly, their corresponding pattern, scan engine version, and `intscan.ini` files must be identical. Additionally, all IWSS servers should use the same database for policy settings and other configuration data.
- Do not delete any table data from the database.
- MSDE 8.00.761 is installed with IWSS.
- To install MSDE on a drive other than the default C: drive, first install MSDE 2000 SP3a from Microsoft (http://www.microsoft.com/sql/msde/downloads/default.asp) on the desired drive. IWSS will detect where MSDE is installed.

- Since deployment conditions may vary, customers are encouraged to consult the IWSS sizing guide, available through Trend Micro sales or support.

Installation Planning

IWSS 2.5 supports upgrading from IWSS 2.0 (see *Upgrading From Previous Versions* starting on page 25).

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

Select the components to install:

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

URL filtering and Applets and ActiveX security each require a separate Activation Code. You also need to choose the type of database to use and whether to run the database on the IWSS server or a separate server:

- MSDE, which is installed with IWSS or
- SQL Server

Also, you need to define your user identification mechanism (see *User Identification Process* starting on page 17 for more details) to use when configuring policies and generating reports:

- Identify by IP address
- Host name (modified HTTP headers)
- User/group name via proxy authorization (that is, LDAP)

Remote Installation

IWSS can be installed to either a local or remote server. To perform a remote install, choose the target servers and enter credentials with local or domain administrator privileges. The setup program then connects to the target servers, copies the installation files, and performs a silent installation.

HTTP Scanning

Choose the type of HTTP handler to use, either:

- HTTP proxy
- ICAP server

Note: If there is already a content cache server on your network, choose ICAP.

The most common installation uses IWSS as a forward proxy to protect clients from downloading risks from the Internet. Configure the HTTP proxy in 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 Settings**) of the IWSS console. See *HTTP Proxy Topology* starting on page 8 for more information. For **Dependent mode**, specify the proxy name and port number. **Dependent mode** requires additional hardware (proxy server); however, it supplements the existing HTTP proxy for other features such as caching, logging, filtering, and network configuration.

FTP Scanning

You can set up the IWSS FTP service (either ICAP mode or HTTP proxy) to run in one of the two settings available:

- Stand-alone: the IWSS server acts as a FTP proxy server
- Upstream FTP proxy: IWSS works in conjunction with another FTP proxy server

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 an upstream proxy).

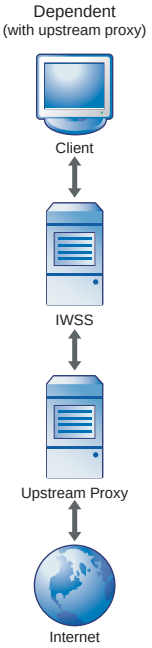


FIGURE 1-1 HTTP proxy in standalone mode (no other proxy)

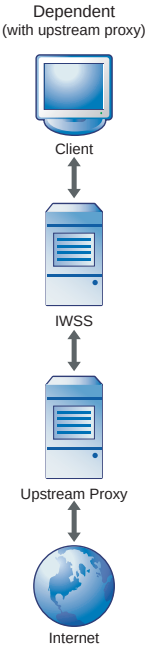


FIGURE 1-2 HTTP proxy in dependent mode (working in conjunction with other proxy)

Forward Proxy

Deploying IWSS as a forward proxy is the most common installation, and helps to protect clients from security risks via HTTP. IWSS and the clients it protects are typically installed within the same LAN.

Transparency Options

To process HTTP requests without needing to change client Internet connection settings, IWSS supports two types of transparency—simple transparency and the Web Cache Communication Protocol (WCCP).

Note: Policies using the "user/group name via proxy authorization" identification option are not supported when transparency is enabled—policies have to be configured based on client IP address or hostname.

Simple Transparency

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

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

Web Cache Coordination Protocol (WCCP)

IWSS supports transparency through routers that support WCCP. When using WCCP transparency, FTP over HTTP connections are supported and FTP downloads are scanned. WCCP v2.0 supports multiple routers, and the WCCP protocol automatically reconfigures for load balancing when IWSS servers are added or removed from your network.

Trend Micro recommends using Cisco IOS versions:

- 12.2(0) to 12.2(22). Avoid using versions 12.2(23) and above.
- 12.3(10) and above. Avoid using IOS versions from 12.3(0) to 12.3(9).

Note: In transparent mode (both simple and WCCP), IWSS does not accept SSL (HTTPS) traffic. Configure the router not to redirect port 443 traffic to IWSS.

Reverse Proxy

IWSS can also be installed as a reverse proxy to protect a Web server from security risks. In the reverse proxy configuration, IWSS is typically installed closer to the Web server that it protects.

Note: For more information about the various proxy and transparency options, including the required product configurations, consult chapter 3 of the IWSS *Administrator's Guide*.

IWSS HTTP Stand-alone Installation with Multiple Servers

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

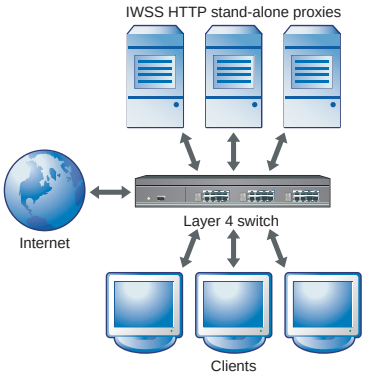


FIGURE 1-3 Use a Layer 4 switch to load balance between IWSS servers for multiple HTTP stand-alone servers

IWSS ICAP Installation with Multiple Servers

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

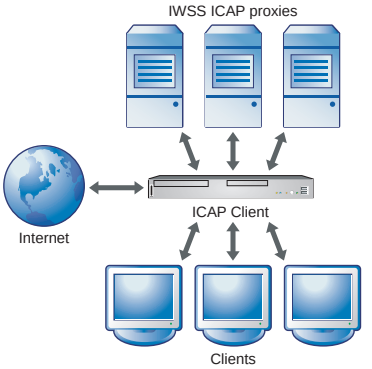


FIGURE 1-4 Multiple IWSS ICAP server installation

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.

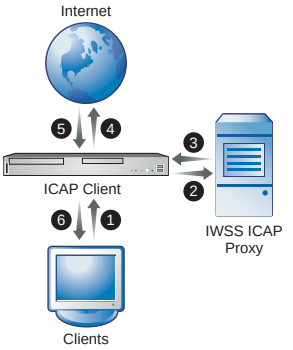


FIGURE 1-5 ICAP request mode workflow

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.

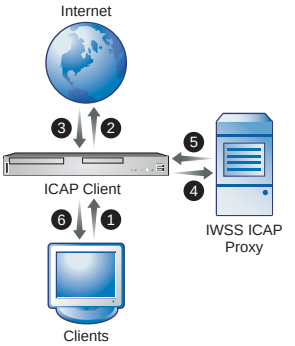


FIGURE 1-6 ICAP response mode workflow

FTP Installation Topology

There are two configuration topologies for FTP scanning:

- 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

Stand-alone Mode

To scan all FTP traffic in and out of the LAN, set up the FTP scanning module so that it "brokers" all such connections. In this case, clients FTP to the IWSS server, supply the logon credentials to the target site, and then 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 and other security risks.

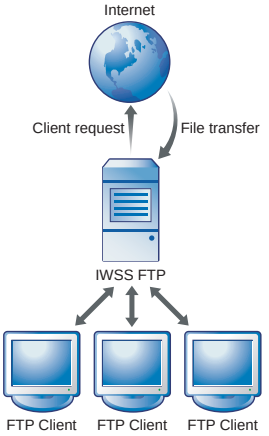


FIGURE 1-7 Configure the FTP proxy setting in the IWSS console

Upstream FTP Proxy

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

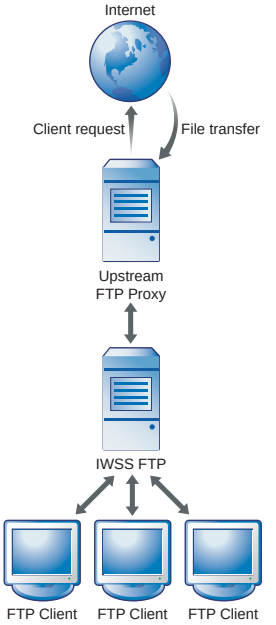


FIGURE 1-8 Using IWSS with an upstream FTP proxy

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

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

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

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

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

The IWSS management console displays the graphs (Bar, Stacked bar, or Line) and statistics of a generated report. In addition, you can export data from IWSS logs for further analysis using Microsoft Excel. To query and generate reports dynamically, IWSS uses an efficient database management system that can support other major databases as a plug-in. The IWSS package includes the Microsoft SQL Server Desktop Engine (MSDE) for the Windows platform. As MSDE has the same database engine as SQL Server, IWSS also supports Microsoft SQL Server 2000. IWSS uses queries that have only been tested for SQL Server and MSDE.

User Identification Process

IWSS uses four user identification methods to configure policies and trace events back to clients:

- No identification (does not identify the client machine for HTTP requests)

- IP address (default setting)
- Host name (modified HTTP headers)
- User/group name via proxy authorization (that is, LDAP)

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

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

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 `INSTALL_PATH/Trend Micro/IWSS/HTTP` folder after the Windows installation.

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** option verifies the user credentials as well as retrieves the group information. The directory service makes the physical network topology and protocols transparent so that a user on a network can access any resource without knowing where or how it is physically connected. LDAP defines a standard method for accessing and updating information in a directory. The

information needed to use a user validation/group retrieval during proxy authorization are as follows:

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

The authentication behavior between IWSS and the directory server differs from the authentication method used between the client browser and IWSS. The authentication method between client browsers and IWSS is explained in Table 1-1. User logon authentication remains secure when choosing simple authentication for the user credential that is passed between IWSS and the directory server. This option uses plain text for the LDAP Admin account credential configured on the LDAP settings page, and this credential is passed between IWSS and the directory server for initial LDAP authentication or connection testing only. During user logon, IWSS still uses the advanced authentication method (not revealing a user's password) when sending the users' credentials between IWSS and the directory server. Secure authentication for the latter depends upon the directory server's vendor, either Kerberos or Digest-MD5.

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

Notes on User/Group Name via Proxy Authorization

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

- IP address: It is impossible to identify the person making a request if multiple users share the same computer, or if IP addresses do not adequately identify the computer where a request originates
- Host name (modified HTTP headers): User/group proxy authorization can be configured in environments where multiple operating systems are used, while the

host name identification method only works on Windows for Web browsing via Internet Explorer

User/group proxy authorization operates effectively in environments where:

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

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

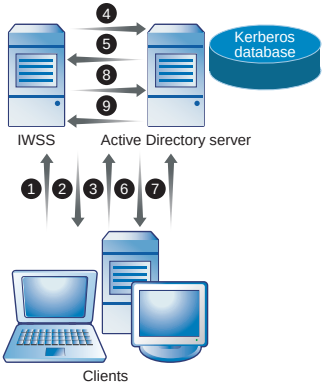


FIGURE 1-9 LDAP server authentication workflows (Active Directory shown)

The authentication workflows for Active Directory are explained below (authentication workflows for other directory servers are similar):

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

9. Active Directory server authenticates the user.

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

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

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

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

TABLE 1-1. 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

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

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

In network environments where IP addresses adequately identify the machines where requests originate, IWSS can use a cache that retains a previously-entered credential for a period of time. The default time-to-live (TTL) for entries in this cache is 15 minutes in HTTP mode and 90 minutes in ICAP mode.

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

Damage Cleanup Services (DCS) Integration

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

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

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

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

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

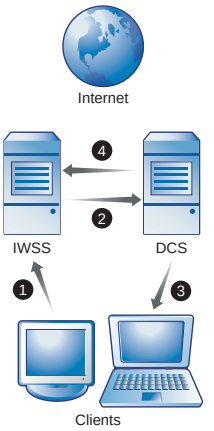


FIGURE 1-10 How IWSS requests DCS to perform a client cleanup

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

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

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

Note: If you are using DCS in conjunction with a HTTPS-enabled IWSS Web management console, IWSS must be configured to allow access to the secure port (typically 8443). If access to the secure port is blocked, IWSS will be unable to redirect clients to DCS for clean-up requests. For more information, see *Using SSL with Damage Cleanup Services (DCS)* starting on page 75.

Upgrading From Previous Versions

The IWSS 2.5 migration program (upgrade.exe) can migrate configuration settings from an existing IWSS 2.0 installation. When the migration program starts installing to a target server, it detects any existing IWSS 2.0 installation and prompts you whether to migrate the settings.

Note: If you install IWSS 2.5 to a server where IWSS 2.0 is installed and choose not to migrate, the previous version settings are lost and cannot be recovered. Additionally, migrating previous version settings requires using the IWSS 2.0 version database—choosing to use another database will not migrate the settings.

When migrating from IWSS 2.0 to 2.5, notification settings (administrator email address, email server host name, and port) and proxy settings for update are migrated to the 2.5 installation if the relevant fields in the setup program are left blank. However, if information is entered into those fields, then the new settings are used. Control Manager server information is not migrated and must be re-entered into the setup program.

Chapter 2

Installing and Removing

This chapter guides you through installing, removing, activating IWSS.

Topics in this chapter include:

- Preparing plans and other environment information needed to install IWSS
- Running the setup program
- Installing and activating IWSS
- Installing or removing IWSS from one or more remote servers
- Opening the IWSS management console
- Obtaining Activation Codes
- Activating the IWSS modules post-install
- Viewing and renewing the maintenance agreement
- Modifying the IWSS installation
- Removing IWSS

Information Needed to Install

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

Type of HTTP Handler

If installing HTTP scanning, you will be prompted to choose the type of HTTP handler to install. Installing IWSS as a stand-alone proxy allows IWSS to act as the network's proxy server or work in conjunction with another proxy. Alternatively, you can install IWSS to act as an ICAP server.

Type of Proxy Configuration

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

Another installation scenario is to configure IWSS as a reverse proxy, to protect a Web server from having malicious content uploaded to it.

Control Manager Server Information

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

Database Type and Location

IWSS uses a database, either the Microsoft SQL Server Desktop Engine (MSDE) or SQL Server, for report logs, policies, rules and configuration settings. Choose to install an instance of MSDE unless you have an existing SQL Server to use.

Notification Email Settings

IWSS sends notifications in response to many security risk detections, policy violations or program events. The setup program prompts for the email address to

send notifications, and an SMTP server that allows message relay from the IWSS server.

SNMP Notifications

If you plan to use SNMP notifications, IWSS can either use the native Windows SNMP agent or the setup program can install another SNMP agent.

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

Management Console Password

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

Proxy for Internet Updates

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

Activation Codes

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

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

Fresh Install or Migration

If installing IWSS as a fresh install, or to not migrate previous version settings, run `setup.exe` (any previous IWSS version should be removed first using Add/Remove Programs in the Windows Control Panel). To migrate 2.0 version settings and remove IWSS 2.0, run the `Upgrade.exe` executable.

Installing InterScan Web Security Suite

Trend Micro recommends installing IWSS on a dedicated server. The IWSS setup program can either install to a local or remote server, and there are two ways to install IWSS:

- Download and run the setup program
- Run the setup program from the Enterprise Solutions CD

Installing from the Enterprise Solutions CD

If you are installing IWSS from the Enterprise Solutions CD, do the following to run the setup program.

Note: Temporarily disable any pop-up blocking software before choosing options on the Enterprise Solutions CD disc.

To run the IWSS setup program from the Enterprise Solutions CD:

1. Start the Enterprise Solutions CD by inserting the disc into the server. If Autoplay is not enabled, browse the disc and open `start.htm` in the disc's root folder.

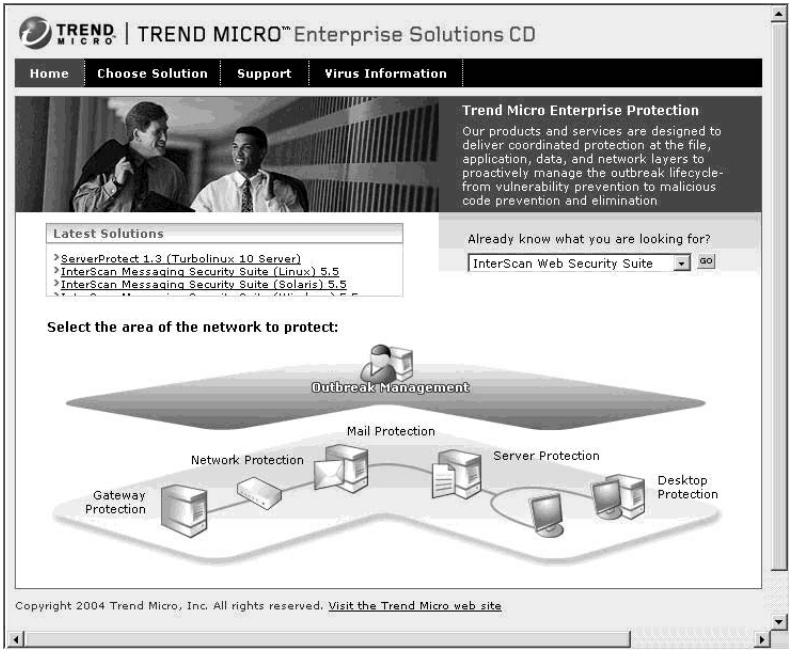


FIGURE 2-1 Select InterScan Web Security Suite from Enterprise Solutions CD Home page

2. Select **InterScan Web Security Suite** from the drop-down on the main page and click **Go**.
3. Select the Windows version, click **Install** and then follow the on-screen instructions.

Running the Setup Program

Copy the IWSS setup files to a temporary folder and complete the following steps to install the software.

Running the IWSS setup program from a folder:

1. Open the folder containing the IWSS setup files in a Windows Explorer window.
2. Double-click the file `setup.exe` to begin installing. The setup program's **Welcome** screen displays.
3. Click **Next**.
4. To install IWSS to the local server, select **Install IWSS on this machine**. If you want to install one or more instances of IWSS to remote servers, select **Install IWSS on one or more remote machine(s)** and see *Choosing and Connecting to Remote Servers* starting on page 48 for more information about selecting the target servers. Click **Next**.

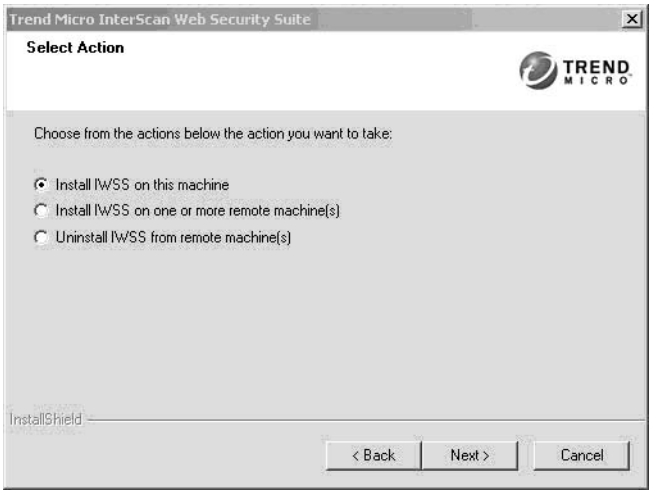


FIGURE 2-2 Choose "Install IWSS on this machine"

5. The **License Agreement** screen displays. Click **Yes** to accept the terms of the license agreement. Click **No** to close the setup program.

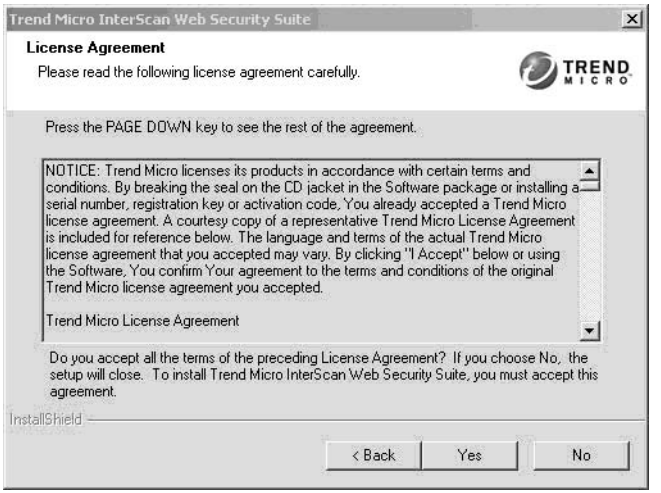


FIGURE 2-3 Click "Yes" to accept the License Agreement

6. The IWSS setup program checks to ensure the server meets the minimum system requirements. Click **Next**.
7. The **Installation Folder** screen displays. Type the path where you want to install IWSS, or click **Browse** to select a folder. The default destination is:

   `C:\Program Files\Trend Micro\IWSS\`

   Click **Next**.

Note: IWSS does not support installation to a shared drive. Either install to a local drive, or install to a remote server using the remote install options (see *Choosing and Connecting to Remote Servers* starting on page 48).

---

8. The **Module Selection** screen displays. Select the modules and features you want to install. Options are:
   - **Main Program**—installs the administration user interface and the basic library files necessary for IWSS

- **HTTP Scanning**—installs the service necessary for HTTP scanning and URL blocking
- **FTP Scanning**—installs the service necessary to scan and block files in FTP transfers
- **URL Filtering**—installs the service necessary to configure policies that manage the types of Web sites clients can view
- **Applets and ActiveX Scanning**—installs the service necessary to check certificate validity of Java applets and ActiveX controls, and instrument applets to permit real-time monitoring on client workstations
- **SNMP Notifications**—installs the service to send SNMP traps to SNMP-compliant network management software in response to security risk detection or program events.
- **Control Manager Agent for IWSS**—installs the files necessary for the Control Manager agent, to enable centralized management, updates, and consolidated logging through Control Manager. You need to install the agent if you are using Control Manager (Trend Micro's central management console). Installing IWSS and Control Manager on the same machine is not supported.
- **Register with Control Manager**—performs the registration process to link the IWSS Control Manager agent to a Trend Micro Control Manager server

9. Click **Next** to continue.

Note: Installing the URL Filtering or Applets and ActiveX Scanning options will require Activation Codes for those modules.

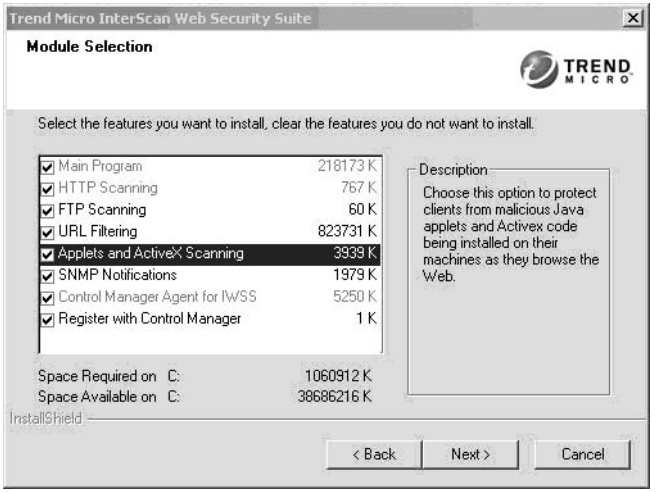


FIGURE 2-4 Select the IWSS modules and features to install

10. If you selected the **HTTP Scanning** module in the **Module Selection** screen, the **HTTP Handler** screen displays. Choose the type of HTTP handler to install:

- **ICAP server** if there is an ICAP-compliant cache server on the network
- **HTTP Proxy** if IWSS will work with another proxy on the network, or serve as a proxy

See *HTTP Proxy Topology* starting on page 8 for more details. Click **Next**.

11. If you selected to install the **HTTP Scanning** module, you need to decide on the type of proxy configuration:

- **Forward Proxy** is used to protect clients on the network from malicious Internet downloads. When installing IWSS as a forward proxy, you can also choose among several transparency options. Transparency is the functionality whereby client users don't have to change their Internet connection's proxy settings to work with IWSS by using a layer 4 switch.
  - **Simple transparency** is supported by most layer 4 switches

- **Web Cache Coordination Protocol (WCCP)** is a protocol defined by Cisco Systems, Inc. that supports multiple routers and automated reconfiguration for load balancing on routers when adding or removing IWSS servers.

- **Reverse Proxy** is used to protect a Web server from receiving malicious content that clients might upload to it

  For more information, see *HTTP Proxy Topology* starting on page 8 and *Transparency Options* starting on page 9. Check the type of transparency to use and then click **Next**.

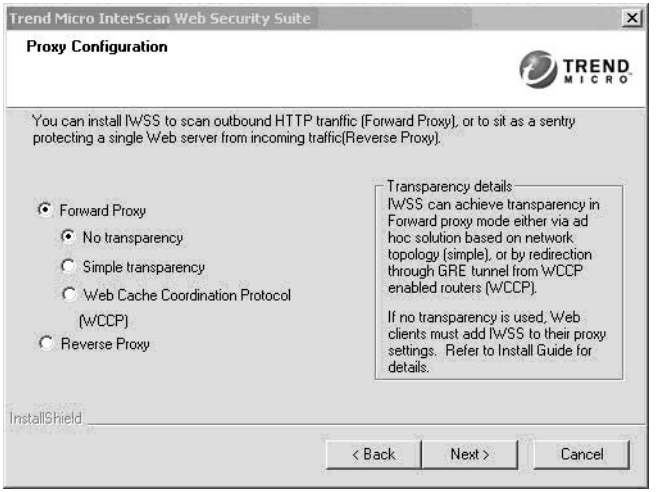


FIGURE 2-5 Select the type of HTTP proxy

12. If you selected **Register with Control Manager** in step 8, the **Control Manager Agent Setup** screen displays. Type the host name (or IP address) and the port number of the Control Manager server. Click **Next** to continue.

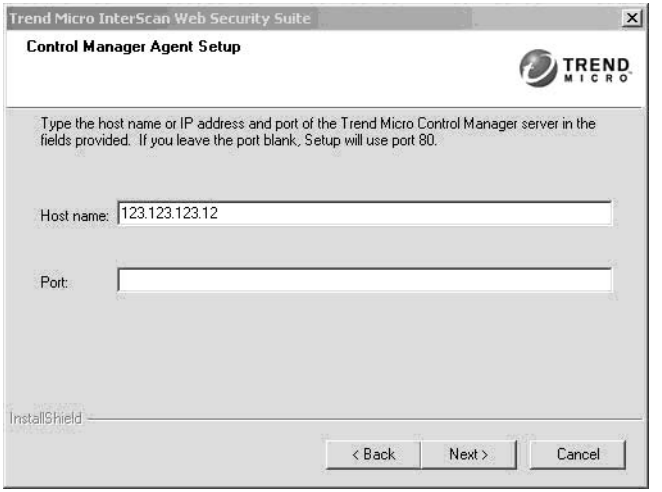


FIGURE 2-6 Enter the Control Manager server's IP address or host name

13. In the **Control Manager Administration Account** screen, type the Control Manager logon name and click **Next**.
14. Choose the type of database to use for report logs, policies, rules, and quota consumption information. The default option is to have the IWSS setup program install the Microsoft SQL Server Desktop Engine (MSDE). If you want to use an

existing Microsoft SQL Server database, check **Other**, choose the **Database** and select the type of authentication. Click **Next**.

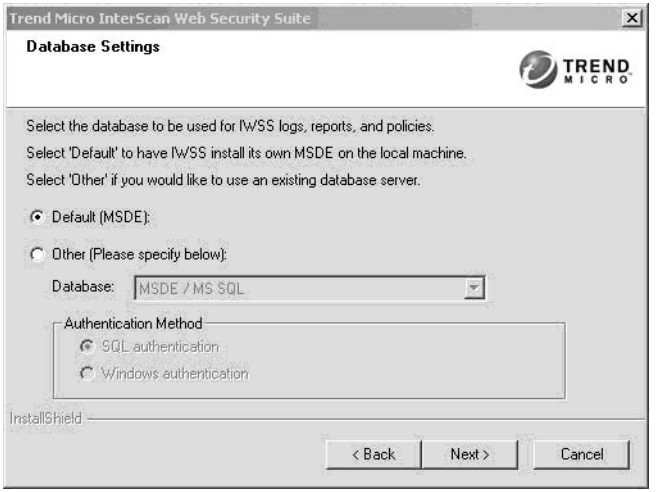


FIGURE 2-7 Choose the type of database and authentication method

15. In the **ODBC Data Source** screen, specify or create a DSN of the database with which IWSS will communicate (default = “IWSS”), for either a new or existing

database. The default **User name** is “sa”. Enter a password for the database connection. Click **Next**.

FIGURE 2-8 Enter the database’s DSN and authentication credential

16. IWSS can send notifications in response to scanning, file blocking, URL blocking, malicious Applet and ActiveX events and updates. Enter the **Email** address, and the **Host name** and **Port** of the SMTP server to use for sending

notifications. The SMTP server that you specify must allow relay from the IWSS machine (remember to configure your mail server accordingly).Click **Next**.

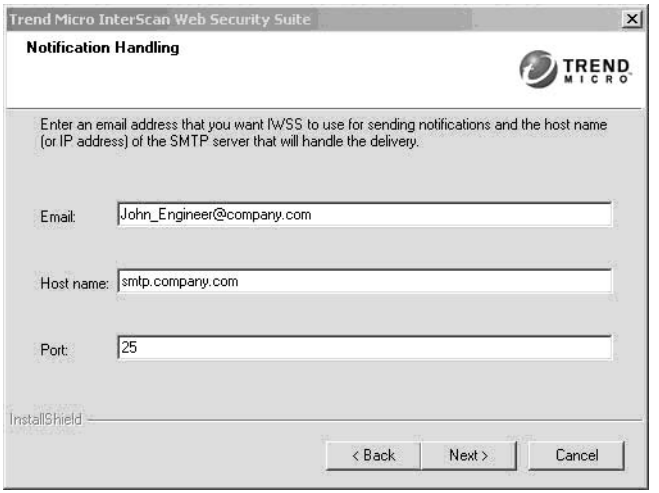


FIGURE 2-9 Enter the email address and SMTP server to send notifications

17. IWSS can send notifications to SNMP-compliant network management utilities in response to program or risk events. To have IWSS install an SNMP agent,

select **Default**. If the target server where you're installing IWSS already has the Windows SNMP agent, check **Other**. Click **Next**.

FIGURE 2-10 Select the type of SNMP agent for notifications

18. In the second **SNMP Configuration** screen, enter the settings for SNMP-related objects allowed to query the IWSS SNMP agent. You can specify the SNMP-related settings for objects that will have read and write, or read only access.
    - Community name: The SNMP community string
    - Host name: The object's host name
    - Object identifier (OID): A long numeric tag, used to uniquely distinguish each variable in the Management Information Base (MIB) and in SNMP messages, e.g., 1.3.6.1.2.1.1.5.0

You can send an authentication trap, if the object requires it. Click **Next**.

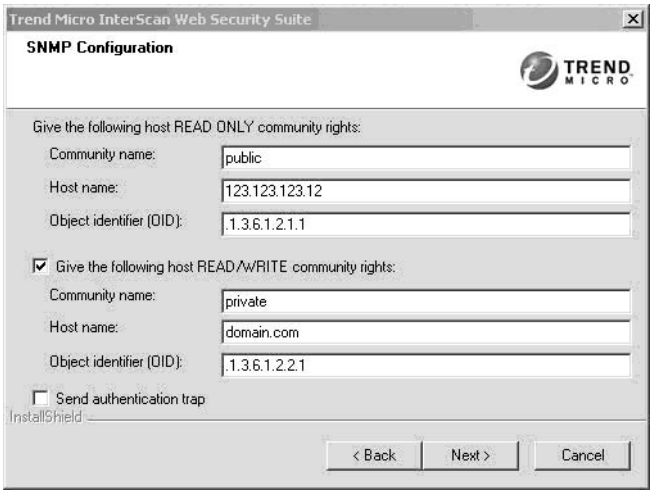


FIGURE 2-11 Enter SNMP configuration settings

19. Enter the settings for the SNMP manager that will receive SNMP traps from the IWSS SNMP agent. Type the **Location** and **Contact** person if required by the

manager. Type the **Host**, **Community name** and **Port number** of the manager that will receive the traps.

FIGURE 2-12 Enter SNMP-compliant device to receive notification traps

20. Enter the password (between 4 to 32 characters) to restrict IWSS management console access. Click **Next**.
21. In the **Connection Settings** screen, specify how you access the Internet to activate and update the software. If Internet connections pass through a proxy server, enable **Use a proxy server to connect to Internet**, and then type the

address and port number of the proxy server. If the proxy server requires authentication, enter the **User name** and **Password**.

FIGURE 2-13 Enter proxy server details to download pattern and program updates (if necessary)

22. Next, the **Product Activation** screen displays. The Registration Keys that came with your IWSS purchase are exchanged for Activation Codes during product registration. The Activation Codes are used to unlock full, that is, non-evaluation, versions of the IWSS modules. Click the **Register Online** button to visit Trend Micro's online registration Web site to register IWSS and

obtain Activation Codes. Once you have Activation Codes, enter them into appropriate fields

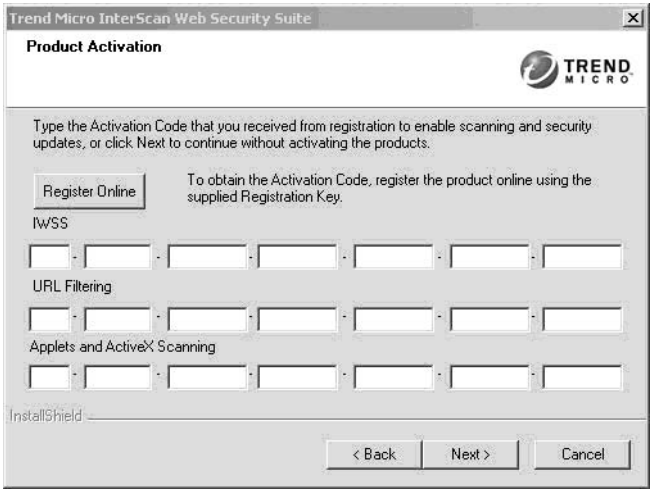


FIGURE 2-14 Enter Activation Codes for selected modules

If you have the Activation Code(s), type them in the fields provided. Enter Activation Code(s) for the modules that you are installing: IWSS, URL Filtering and/or Applets and ActiveX Scanning. Alternatively, you can leave these fields blank to install evaluation versions and activate the installation from the management console after you have completed installation.

Note: Security updates, scanning and filtering capabilities will be enabled after activation.

---

23. With customer authorization, Trend Micro collects and consolidates infection data from product installations worldwide. These transmissions contain infection data and no user-specific information is sent. This data is used to generate the Virus Map on the Trend Micro Web site

(`http://www.trendmicro.com/map/`). If you would like to participate in this program, select **Yes**. Click **Next**.

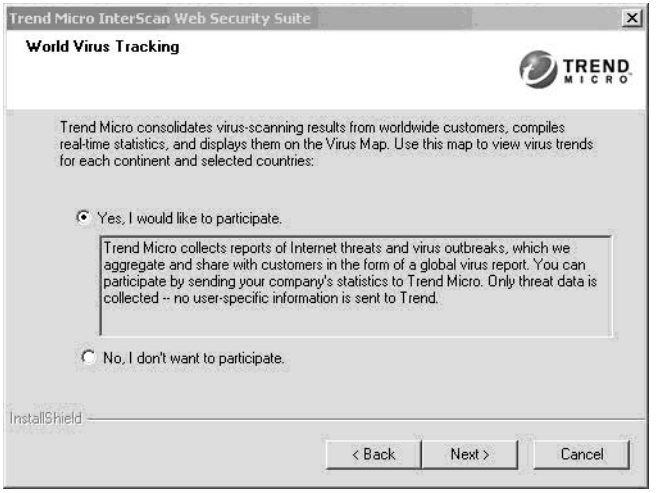


FIGURE 2-15 Select Yes to participate in the World Virus Tracking program

24. The setup program now has enough information to install IWSS. Review the summary of settings in the **Settings Review** screen and then click **Next** to start copying files.

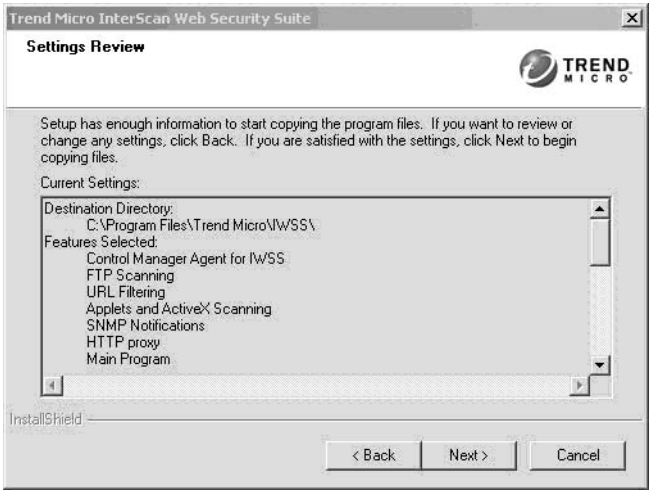


FIGURE 2-16 Review the installation choices

25. A progress bar and status messages are displayed as the IWSS files are copied to the target server. When file copying concludes, you must restart the server to

finish the installation progress. Check the options to display the readme file and open the management console after the server restarts. Click **Next**.

FIGURE 2-17 View the readme for late-breaking product information

26. The **InstallShield Wizard Complete** screen displays. To restart the computer, check **Yes** and then click **Finish**.

Choosing and Connecting to Remote Servers

If you need to install or remove an installation from a remote server, the setup program needs to know the server's identity and a credential with local or domain administrator privileges to connect to it.

1. Select the servers upon which you want to install or remove IWSS. You can enter the servers in one of the following ways:

- Drill down into the Windows domains displayed in the left-hand pane, select the host name and click **Add**.
- Type the IP address or host name into the **Add server name** text box and click **Add**.

When the right-hand pane shows all the servers that you want to select, click **Next**.

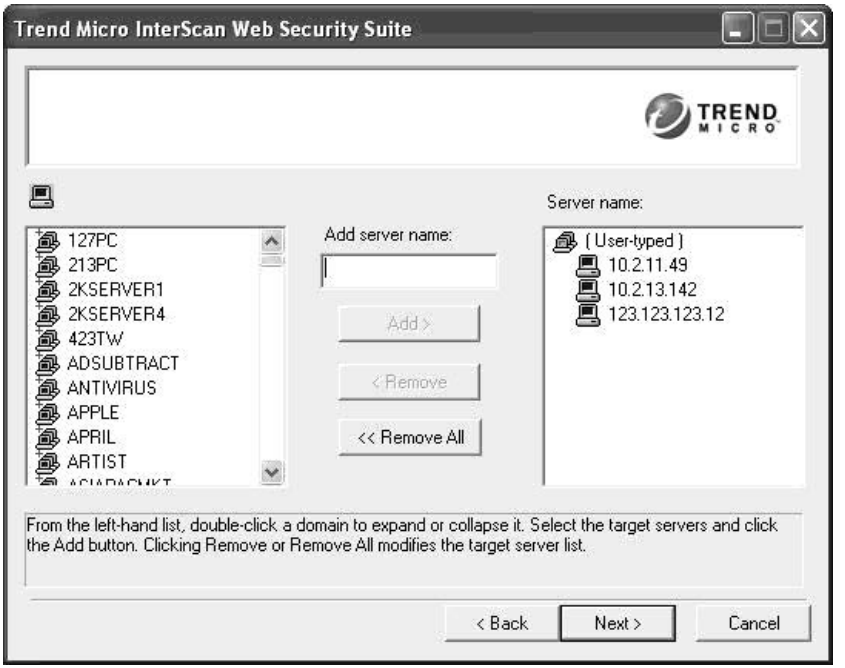


FIGURE 2-18 Select or type the remote servers

2. To install or remove IWSS, you need to enter a credential with local or domain administrator privileges to the IWSS server. Type the **User name** and **Password**. If you want the InstallShield Wizard to save your credential after a successful

logon and use it for successive installs or removals, select **Remember user name and password if logon succeeds**. Click **Logon**.

FIGURE 2-19 Enter credential with local or domain administrator privileges to the target servers

3. A screen loads to display the logon process, and the result. If you were able to log on successfully using the credential that you entered, click **Next**. Otherwise, click **Back**.

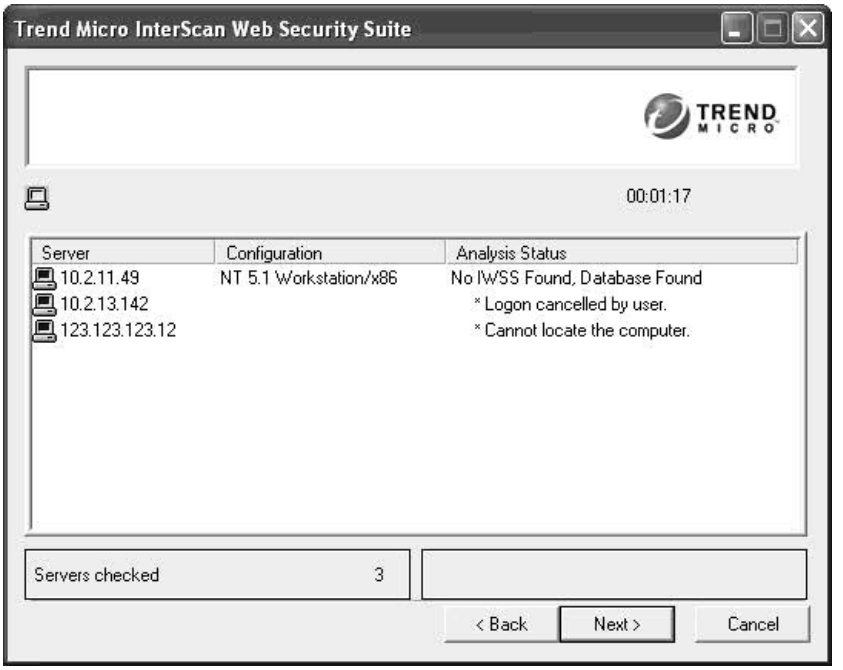


FIGURE 2-20 Review the results of the remote logon attempts

Note: If the remote analysis results conflict with the intended action, for example, the administrator wants to install using a SQL server database but MSDE is already installed on the server, click **Back** to remove the server from the list or reconsider the installation/removal options.

4. After connecting to the remote servers, the setup program then proceeds with the installation or removal. A summary screen is presented showing the status of all install or removal attempts.

Migrating Previous Version Settings

If there is already an IWSS 2.0 installation on the network, run `Upgrade.exe` to migrate version 2.0 settings to IWSS 2.5 and remove version 2.0.

Opening the IWSS Management Console

To open the IWSS console:

1. Do one of the following:
   - From the computer where you installed IWSS, choose **Start** > **Programs** > **Trend Micro IWSS**> **IWSS Web UI** > **Administration Interface**.
   - Open a browser window and type the URL of the IWSS management console. You can either enter the URL using the qualified domain name, machine name or IP address. For example,

     `http://domain:port/index.jsp`

     `http://<machinename>:1812/index.jsp`

     `http://123.123.123.12:1812/index.jsp`
2. Type the management console password that you configured during installation and click **Enter**. The management console will open to the **Summary** page.

See *Encrypting Browser-Console Communication (HTTPS)* starting on page 72 for information on how to access the IWSS console via HTTPS.

Activating the Installation

If you did not activate IWSS during installation, activate the modules using the IWSS management console after installation. The HTTP scanning, URL filtering and Java applet and ActiveX scanning modules each need their own Activation Codes.

To activate installed IWSS modules, or update the Activation Code:

1. From the main menu, click **Administration** > **Product License**.
2. The **Product License** screen displays license status information for the installed IWSS modules.

3. Click the **Enter a new code** link next to the module to activate and type in the Activation Code.

FIGURE 2-21 Enter an Activation Code for the installed module

4. Click **Activate**.
5. Click **Product License** on the main menu to return to the **Product License** screen and repeat steps 3 and 4 for any other modules that you want activate or update.

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 at Trend Micro's online registration Web site (`http://olr.trendmicro.com`)

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 entitles you to the following benefits:

- Updates to the virus pattern file, spyware and PhishTrap pattern files and the 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 the 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 the product.

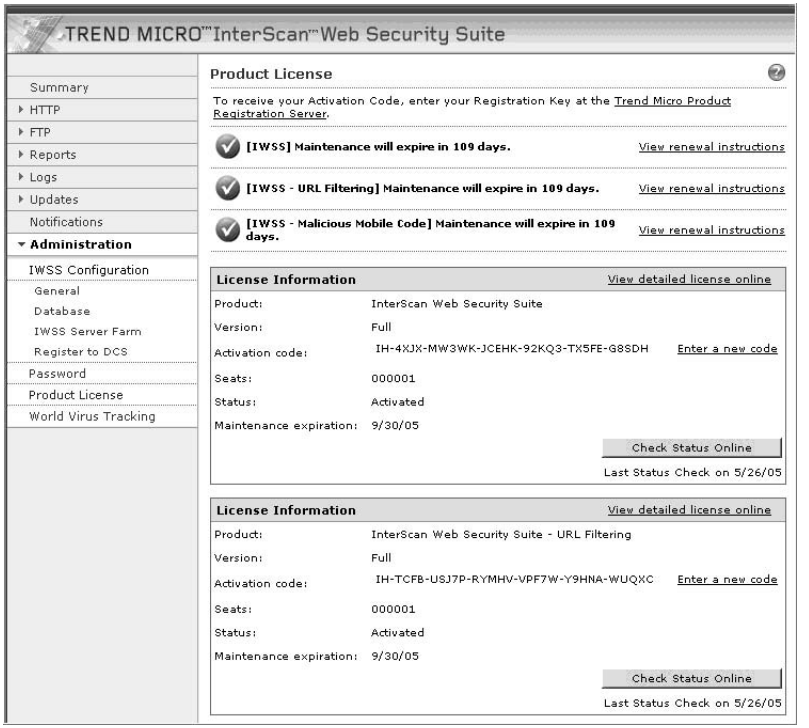


FIGURE 2-22 Review license information in the "Product License" screen

To obtain an Activation Code online:

1. Open the IWSS console and click **Administration** > **Product License**.
2. Click **Trend Micro Product Registration Server**
3. When the Online Registration Web site loads, follow the onscreen instructions to register the purchase.

Maintenance Agreement

A Maintenance Agreement is a contract between the customer and Trend Micro, regarding the 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. The 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 expiry. You can update the Maintenance Agreement by purchasing renewal maintenance from the reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

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

Renewing the 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 the 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 protection for a year, will be sent by post to the primary company contact listed in your organization's Registration Profile.

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

`http://olr.trendmicro.com`

You are prompted to enter a logon ID and password.

FIGURE 2-23 Renew the license agreement at the Trend Micro Online Registration site

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

Modifying an IWSS Installation

To modify the IWSS installation, you need to run the maintenance program from the server where IWSS is installed.

To modify an IWSS installation:

1. Do one of the following to start the maintenance program:
   - Run **Start > Settings > Control Panel > Add/Remove Programs**, select the Trend Micro InterScan Web Security Suite entry and then click **Change/Remove**.
   - Navigate to the disc or drive that contains the IWSS setup files and run the setup program. The setup program will detect the existing product installation.
2. The **IWSS Maintenance** window loads. Select **Modify IWSS installation on this machine** and click **Next**.

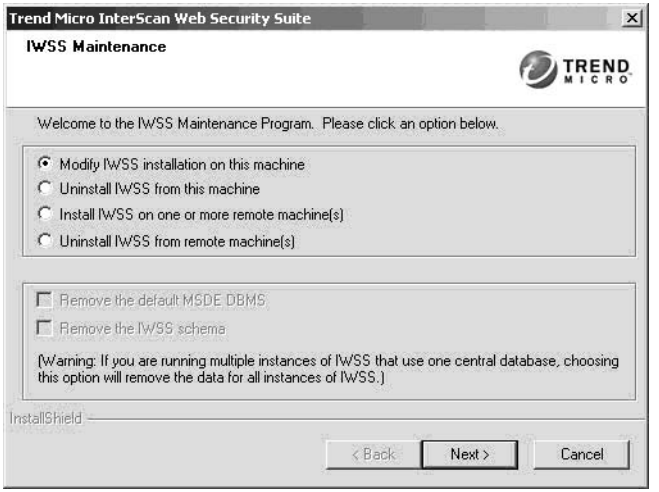


FIGURE 2-24 Select the maintenance operations to perform

3. The **Select Features** window opens. Select the modules and features to install, or clear the ones to remove. Click **Next**.

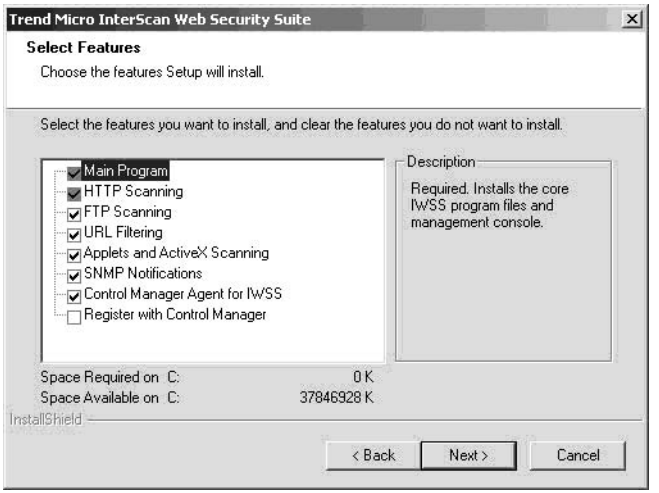


FIGURE 2-25 Select modules and features to add or remove

4. Depending on the features selected, the maintenance program will display additional windows to enter feature-specific configuration settings. For more information about these screens, see their description under *Installing InterScan Web Security Suite* starting on page 30. The following are the installation steps that pertain to a given feature:
   - HTTP Scanning: steps 10 and 11 starting on page 35
   - FTP/Applets and ActiveX Scanning and URL Filtering: step 22 on page 44
   - SNMP Notifications: steps 17, 18 and 19 starting on page 40
   - Register with Control Manager: steps 12 and 13 starting on page 37
5. After performing the modifications that you requested, the IWSS service is restarted and the **Maintenance Complete** window is displayed.

Removing IWSS

The uninstallation program can remove both local and remote IWSS installations.

To remove IWSS from a local machine:

1. From the Windows taskbar, select **Start > Settings > Control Panel** and double-click **Add/Remove Programs**.
2. Find the **Trend Micro InterScan Web Security Suite** entry and click **Change/Remove**.
3. Check **Remove IWSS from this machine** in the **IWSS Maintenance** window. Optionally, select **Remove the default MSDE DBMS** and/or **Remove the IWSS schema**. Click **Next**.

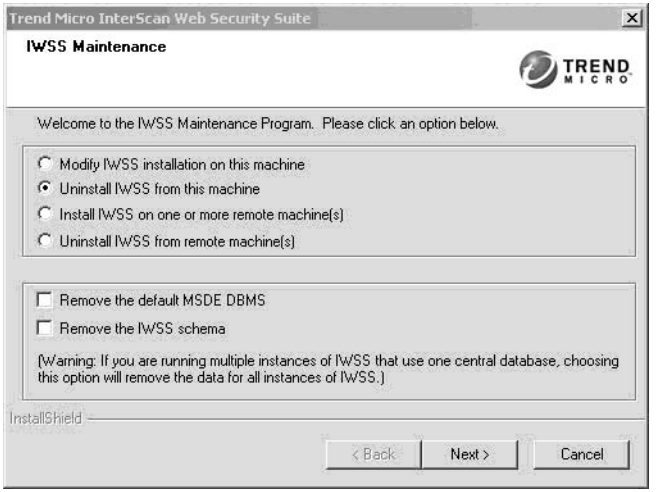


FIGURE 2-26 Select "Uninstall IWSS from this machine"

4. When removal concludes, the **Maintenance Complete** window displays.

To remove an instance of IWSS from a remote server:

1. Browse to the drive or folder where the IWSS setup files are located and run the setup program. The InstallShield Wizard **Preparing to Install** and **Welcome** screens load. Click **Next**.

FIGURE 2-27 Click Next to advance the IWSS maintenance program

2. Select **Uninstall IWSS from remote machine(s)** and click **Next**.

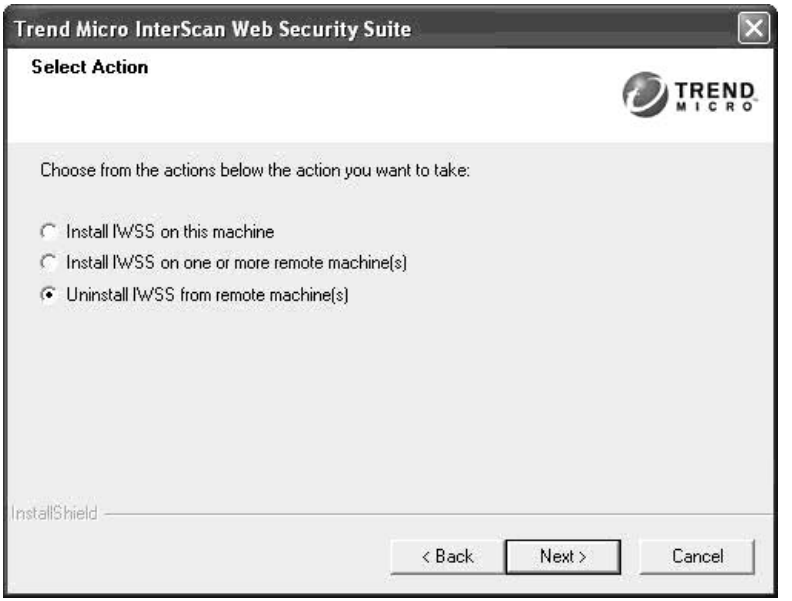


FIGURE 2-28 Choose "Uninstall IWSS from remote machine(s)"

3. The setup program needs to know the servers from which you want to remove the software, and need credentials with local or domain administrator privileges to connect to each one. For more information and screen shots of the remainder of the remote uninstall process, see *Choosing and Connecting to Remote Servers* starting on page 48.

Chapter 3

Post-Installation Configuration

This chapter briefly introduces configuration tasks after installing IWSS.

Topics in this chapter include:

- Enabling HTTP traffic flow through the IWSS server, choosing the user identification method, and configuring proxy scan settings
- Updating program components and keeping IWSS current with hot fixes, patches, and service packs
- Enabling access quota policies, configuring notifications, and enabling the guest account and port
- Configuring URL blocking and improving scanning performance by adding trusted URLs that will not be scanned
- Testing the main IWSS components
- Setting the server's role in a multi-IWSS installation
- Understanding post-installation tasks for IWSS ICAP
- Protecting your IWSS configurations by encrypting browser-console communication and changing the management console password

HTTP Scanning and General Configuration

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

Enabling the HTTP Traffic Flow

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

To enable the IWSS HTTP traffic flow:

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

Configuring the User Identification Method

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

To configure the user identification method:

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

Enabling the Guest Account (LDAP only)

When using the **User/group name via proxy authorization** identification method, virus scanning, Java applets and ActiveX security, URL filtering, and access quota policies all support configuring policies for users temporarily visiting your network. These guest policies are applied to clients that connect to IWSS via the "guest" port. The guest account is disabled in the default post-install settings—enable it to allow guests Internet access.

To enable the guest account and configure the guest port:

1. Click **HTTP > Proxy Scan Settings** from the main menu.
2. Select **Enable guest account**.
3. The default **Guest port number** is 8081 and typically does not have to be modified unless the port is already in use.
4. Click **Save**.

Reviewing Scanning and Filtering Policies

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

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

Updating Program Components

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

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

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

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

1. Click **Summary** on the main menu and make sure the **Scanning** tab is active.
2. For all of the components listed on the **Scanning** tab, select components to update and click **Update**.

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

Reviewing Default Settings

The default IWSS post-install settings are summarized under *Default Post Install Configuration Settings* starting on page 78. These settings provide a baseline level of content security that may be appropriate for your organization. Trend Micro recommends that you carefully review the default settings and modify them according to the security needs of your unique environment and overall security goals.

Enabling Access Quota Policies

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

To enable access quota control:

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

Configuring Trusted URLs

To minimize performance issues from HTTP scanning, Trend Micro recommends configuring "trusted" URLs to exempt from scanning. For example, if you have

configured IWSS in a forward proxy configuration and are confident that your company's Web site does not harbor any security risks, consider adding it as a trusted site. Other reputable Web sites that are frequently visited by your clients, for example, financial Web sites that provide your company's stock quote, can also be configured as "trusted".

To configure trusted URLs

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

Configuring URL Blocking

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

To block URLs:

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

Setting Access Control Settings

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

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

To configure which clients are allowed to access the Internet:

1. Click **HTTP > Configuration > Access Control Settings** from the main menu.

2. On the **Client IP** tab, select **Enable HTTP access based on client IP** and enter the IP addresses that are allowed to access the Internet.
3. On the **Server IP White List** tab, configure the IP addresses of servers that will be exempted from scanning, URL filtering, and URL blocking.
4. Click **Save**.

Configuring Proxy Scan Settings

During installation, the setup program prompts whether to install IWSS as a forward or reverse proxy. If installing as a forward proxy, the setup program also prompts whether to enable transparency.

The type of proxy can be modified in the IWSS console, along with several other proxy-related settings such as the email address for anonymous FTP logon over HTTP, the number of threads, and the number of concurrent connections to the IWSS server. For detailed information, consult the IWSS *Administrator's Guide*.

To modify your proxy settings:

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

Configuring Notifications

The IWSS setup program prompts for an email address and SMTP server to use for update and security event notifications. Also, IWSS is pre-configured with the SNMP settings entered during setup if you installed the SNMP Notifications module.

To review and modify your notification settings:

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

Setting the Database Connection

Make sure that you set up your database appropriately under the **Database Connection Settings** section (**Administration > IWSS Configuration > Database**). When you are setting up a database for multiple IWSS server configurations, specify the same database for all IWSS servers. Whether you are using MSDE or SQL Server for the 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 management console and click **Administration > IWSS Configuration > Database**.
2. Under **Database Connection Settings**, type a value for the following parameters:
   - **ODBC data source name**
   - **User name**
   - **Password**
3. Click **Save**.

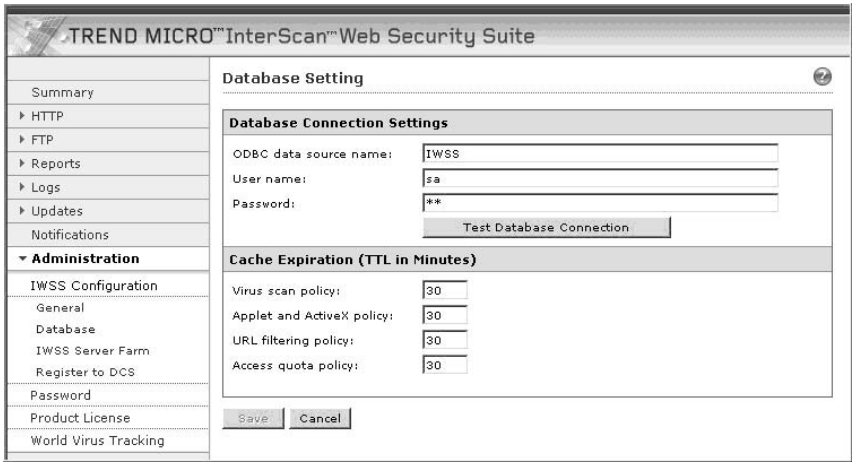


FIGURE 3-1 To verify that the database connection is working, click Test Database Connection

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

To configure Time to Live (TTL):

1. Open the IWSS management console and click **Administration > IWSS Configuration > Database**.
2. Under **Cache Expiration (TTL in Minutes)**, type a value for the following parameters:
   - **Virus scan policy**
   - **Applets and ActiveX policy**
   - **URL filtering policy**
   - **Access quota policy**
3. Click **Save**.

Sending Infection Data to the World Virus Tracking Center

Trend Micro's World Virus Tracking Center provides real-time data about virus infections worldwide. After combining real-time infection data from Trend Micro product installations, Trend Micro publishes this data to the Virus Map on Trend Micro's Web site:

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

By choosing to send your IWSS infection data to the World Virus Tracking Center, you will be contributing to Trend Micro's efforts to provide real-time infection information to its customers and the general public.

With our customers authorization, Trend Micro products send the following information to the World Virus Tracking Center via encrypted HTTPS:

- virus name
- the number of times the virus was found in the file
- the number of infected machines (always 1 for a gateway product like IWSS)
- a fake sender ID
- a fake machine ID
- the virus pattern file number in use when the virus was detected
- the IWSS product code

- the customer's country code

To send infection data to Trend Micro's World Virus Tracking Center:

1. Choose **Administration** > **World Virus Tracking** from the main menu.
2. Select **Yes** and click **Save**.

You can stop sending infection data to Trend Micro at any time by returning to the **World Virus Tracking Program** configuration page and selecting **No**.

Configuring the Quarantine Directory

During installation, IWSS creates a quarantine directory (default path = `C:\Program Files\Trend Micro\IWSS\quarantine`) to copy files in response to a security event:

To modify the quarantine directory:

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

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

Binding to a Network Interface Card

If the server where you installed IWSS has multiple network interface cards, IWSS will listen for traffic on all of them. You can restrict IWSS to listen for traffic on a single NIC.

To configure IWSS to listen to a specific network interface:

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

Changing the Management Console Password

The management console password is the primary means to protect your IWSS server from unauthorized changes. For a more secure environment, change the console password on a regular basis and use a password that is difficult to guess.

The following tips will help you design a safe password:

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

To change the console password:

1. Open the IWSS console and click **Administration > Password** in the main menu.
2. Type your current password in the **Old password** field, and then type and confirm the new password.
3. Click **Save**.

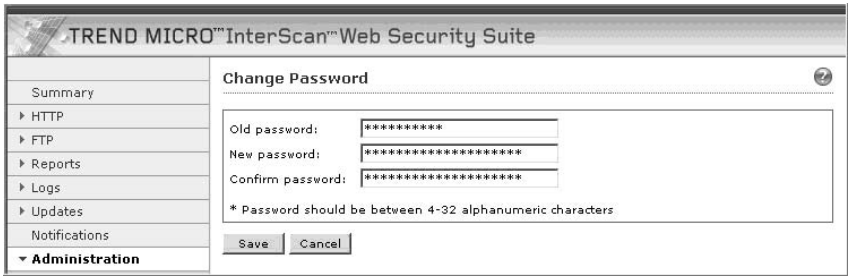


FIGURE 3-2 Use a difficult password (password is case-sensitive) with 4-32 alphanumeric characters

Encrypting Browser-Console Communication (HTTPS)

To prevent the interception of configuration data when it travels from the management console to the server, IWSS can use the secure HTTPS protocol. Tomcat, the Web server that IWSS uses, 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]\AdminUI\jre\bin\keytool.exe` (the default install directory is `C:\Program Files\Trend Micro\IWSS`).

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 `iwss25` as the password.

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

3. Copy `mykeystore` to the Tomcat base directory. (`[Install_directory]\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:

```
[Install_directory]\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="iwss25"/>

</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. Stop and restart the `IWSS_UI` service to enable the certificate.
   Go to **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Component Services** and select **Trend Micro InterScan Web Security Suite Console** under

the **Services (Local)** branch. On the toolbar menu, click **Stop Service**, and then click **Restart Service**.

Accessing the IWSS Console via HTTPS

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

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

```
https://123.123.123.12:8443/index.jsp
```

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

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

```
http://123.123.123.12:1812/index.jsp
```

Disabling Non-HTTPS Access

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

To disable non-HTTPS access:

1. Edit the Tomcat HTTP configuration file:

   ```
   <Install_directory>\AdminUI\tomcat\conf\server.xml
   ```

2. Delete the following nodes:

   ```
   <Connector
   className="org.apache.coyote.tomcat4.CoyoteConnector"
   port="1812" minProcessors="5" maxProcessors="75"
   enableLookups="true" redirectPort="8443"
   acceptCount="100" debug="0" connectionTimeout="600000"
   useURIValidationHack="false" disableUploadTimeout="true" />
   ```

3. Go to **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Component Services** and select **Trend Micro InterScan Web Security Suite Console** under

the **Services (Local)** branch. On the toolbar menu, click the **Stop Service** button, and then click the **Restart Service** button.

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

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

Configurations After Changing the Console Listening Port

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

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

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

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

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

Using SSL with Damage Cleanup Services (DCS)

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

To allow access to secure port 8443:

1. Click **HTTP** > **Configuration** > **Access Control Settings**, and make the **HTTPS Ports** tab active.
2. **Allow** access to the **Port** used for HTTPS traffic (typically 8443).

3. Click **Add** and then **Save**.

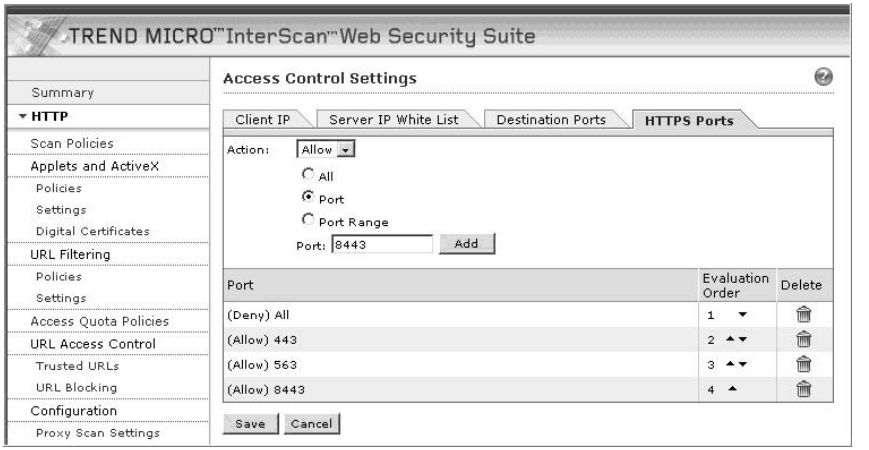


FIGURE 3-3 Allow access to the secure port (typically 8443) if using DCS and the HTTPS management console

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

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

iscan_web_protocol=https
```

URL Filtering

If the optional URL filtering module is installed, review the following post-install tasks to prepare IWSS for your environment.

Verifying URL Filtering Settings

URL filtering is enabled by default and the global policy prohibits accessing URLs that have been categorized to be “company prohibited sites” and “customer defined,” both during “work time” and “leisure time.” IWSS is pre-configured to include URLs that are classified into sub-categories relating to illegal drugs, violence or adult-oriented subject matter as “company prohibited sites.”

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

To review URL filtering settings:

1. Click **HTTP > URL Filtering > Settings** from the main menu.
2. On the **URL Categories** tab, verify that the sub-categories are classified correctly. Move a sub-category to a different classification by selecting it, choosing the classification to which you want to move it, and click **Move**.
3. On the **URL Filtering Exceptions** tab, enter or import Web sites to exempt from URL filtering so that they will always be accessible to your clients.
4. On the **Schedule** tab, the default setting for "work time" is Monday to Friday, from 8:00AM to 11:59AM, and from 1:00PM to 5:00PM. Modify these time settings according to employee schedules in your workplace.

Java Applet and ActiveX Scanning

Java applet signatures are verified using root certificates installed during IWSS setup—to see the list of root certificates, select **HTTP > Applets and ActiveX > Digital Certificates** from the main menu. ActiveX signatures are verified against the root certificates in the IWSS server's Windows certificate store.

Adding Certificates for Applet Signature Verification

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

To add a certificate to the IWSS certificate store:

1. Click **HTTP > Applets and ActiveX > Digital Certificates** from the main menu.
2. On the **Active Certificates** tab, click **Add**, select the certificate and then click **Add**.

3. Return to the **Manage Digital Certificates** screen and verify the added certificate displays in the list.

Default Post Install Configuration Settings

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

Configuration	Default Post-Install Settings
General settings	• HTTP traffic is on • FTP traffic is on • HTTP and FTP virus scanning, Java applets and ActiveX security, URL blocking and URL filtering are all enabled • Guest account is disabled (thus all guest policies are disabled) • IP address identification method is enabled • Quarantine folder is set to \IWSS\Quarantine in the install folder
HTTP virus scanning	The default global and guest policies are configured as follows: • No files are blocked • All files are scanned **Compressed file scanning settings**: The following compressed files are blocked: • Containing more than 10000 files • Decompressed file size greater than 200MB • More than 10 compressed layers • Decompressed size 100 times greater than compressed file size **Large file scanning**: • Files greater than 2048MB are not scanned • Files greater than 512KB are scanned using deferred scanning **Virus scanning actions**: • Infected files are cleaned • Uncleanable files are deleted • Password-protected files are quarantined • No special action for files containing macros **Miscellaneous settings**: • Quarantined files are encrypted • No special scanning for spyware/grayware

Configuration	Default Post-Install Settings
Java applet security rules and settings	**Signature validation**: • Valid signature, trusted certificate: Applet is passed • Valid signature, blacklisted certificate: Applet is blocked • No signature: Applet is instrumented • Invalid signature: Applet is blocked • Applet signatures are validated by checking expiration of signing certificate • Certificates that cannot be verified as trusted have their signatures stripped **Allowed applet operations**: • Connecting to originating servers **Disallowed applet operations**: • Destructive and non-destructive operations • Writing or reading data to local disks • Binding to local ports **Miscellaneous**: • Applets cannot create new thread groups • Applets can create active threads (max 8) • Applets can create active windows (max 5) • Applets are left unsigned after instrumentation
ActiveX security rules and settings	• *.cab files, PE files (*.exe, *.ocx): Verify signatures and block invalid signatures • Expiration of signing certificate is checked
URL filtering policies	• URL filtering is enabled • Global and guest policies block “company-prohibited sites” (sites related to illegal drugs, violence and racism and adult-oriented content) and “customer defined“during work and leisure time • Work time defined to be 8:00AM to 11:59AM and 1:00PM to 5:00PM, Monday to Friday
Access quota policies	• none
URL blocking	• URL blocking is enabled • All URLs in the PhishTrap pattern (phishing, spyware, virus accomplice and disease vectors) are blocked

Configuration	Default Post-Install Settings
FTP scanning	• FTP scanning is enabled (for both upload and download scanning) • No file types are blocked • All files are scanned **Compressed file scanning settings**: The following compressed files are blocked: • Containing more than 10000 files • Decompressed file size greater than 200MB • Containing more than 10 compressed layers • Decompressed size more than 100 times the compressed file size **Large file scanning**: • Files greater than 1024MB are not scanned • Deferred scanning is enabled for files greater than 512KB **Miscellaneous**: • Quarantined files are encrypted • No scanning for spyware/grayware • Infected files are cleaned if possible, otherwise deleted • Password-protected files are quarantined • No special action against macro-containing files
Reports and Logs	• Daily, weekly and monthly consolidated reports for all users are enabled • Reporting logs are written to the database only, and kept for 30 days • Reporting logs include performance data • System logs are written to the \IWSS\Log folder, and kept for 5 days
Updates	• Check for virus, spyware, and PhishTrap pattern updates hourly • Check for scan engine updates weekly • Check for URL filtering database updates weekly
Notifications	**Enabled email notifications**: • HTTP file blocking events • URL blocking events • Virus, PhishTrap, spyware pattern updates and URL filtering database (both successful and unsuccessful) **Disabled email notifications**: • HTTP scanning events • Malicious Java applet and ActiveX events • FTP notifications are on by default
Damage Cleanup Services	• DCS is enabled (but must configure IP address and port of DCS server) • Client browsers are redirected to DCS if cleaning fails

Configuring an IWSS Server Farm

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

To configure server designation:

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

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

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

5. Click **Save**.

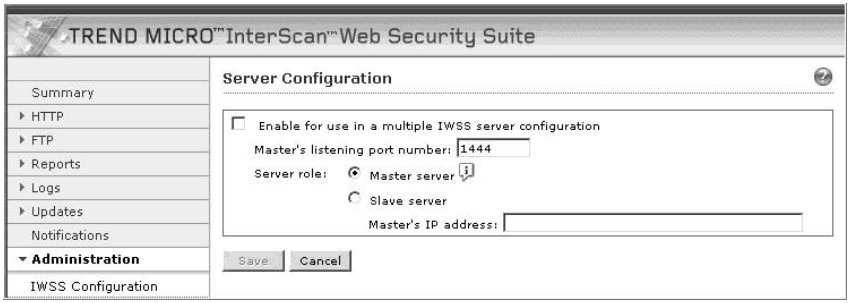


FIGURE 3-4 Configuring the server's role, either master or slave, in the Server Configuration screen

Windows Authentication for SQL Server 2000/MSDE

The following are some guidelines to help configure IWSS to use Windows authentication. Note that the examples do not provide the most secure configuration and will focus on using an Active Directory account. For more details related to SQL Server and Windows authentication, refer to:

`http://databasejournal.com/features/mssql/article.php/3349561`

Note: There are 3 types of Windows user account (local Sam database account, Windows NT 4.0, and Microsoft Windows Active Directory 2000/2003).

Before Installing SQL Server and IWSS

Before installing SQL Server and IWSS, take note of the following:

1. Join the SQL Server/MSDE and IWSS server machines to a domain that can authenticate a user logon to either machine. If the two machines join two different domains, there should be a trust relationship between the two domains.

   Example: Consider a SQL Server that belongs to domain A, and an IWSS server that belongs to domain B. There should be a trust relationship between domain A and B.

2. The user credential, for example, *UserA*, used to log on to the server to install SQL Server/MSDE or IWSS should belong to an Administrative group with permissions to administer the local computer. In this illustration, a user account that belongs to the same domain (domain A) will be used, and this domain user should be manually added to the "Administrators" group to have complete and unrestricted access to the computer/domain group where the IWSS server resides. *UserA* is also a member of Administrators group on domain A.

Install and Configure IWSS and SQL Server/MSDE

1. Install SQL Server 2000.
   a. Use a logon account, for example, *UserA*, with the correct administrative privilege to log on to the SQL Server machine.

b. Install SQL Server.

c. Choose **Use a Domain User account** for the Service Accounts setting during SQL Server setup. Supply the username (*UserA*), password, and domain (Domain A) as the user credential for both IWSS and the SQL Server logon.

d. Select **Mixed Mode** (Windows authentication and SQL Server authentication) during the install.

2. Install the IWSS Server.

a. Use a logon account with administrative privileges to the server where you will install IWSS. For illustration purposes, assume the domain user account is part of the local machine administrative group that has unrestricted access to the computer. The domain user account is also a member of the Administrators (DomainA/Builtin) group of Domain A with unrestricted access to machines in the domain.

b. Run IWSS Setup.

c. Use **Other** (that is, the existing SQL server), then select **Windows authentication**.

d. During installation, enter the FQDN (Fully Qualified Domain Name) of the SQL Server to use as the IWSS database server on the **Database Server** page.

e. Wait for the IWSS Server to restart before proceeding to the next section.

Note: The IWSS server has to be able to resolve the FQDN of the SQL server, and this should be verified prior to installing IWSS.

---

3. Configure SQL Server/MSDE to work with IWSS.

a. Once the IWSS database is created on the SQL Server from the SQL Server Enterprise Manager, create a new login from **Security > Logins**.

Note: The DomainA\UserA used for user logon appears in the **Local > Databases > Security > Logins** dialog box after installation.

---

b. On the **General** tab, ensure the new logon contains DomainA\IWSSservername$ in the **Name** field. Use the default **Windows Authentication** and **Grant access** settings.

c. Select IWSS from the **Database** menu located at the bottom of the **SQL Server Login Properties - New Login** page.

d. Switch to the **Server Roles** tab, and check **Database Creators** and **Bulk insert Administrators**.

e. Switch to the **Database Access** tab, and check "iwss" under the **Database** column. Check "public", "db_owner", "db_datareader", and "db_datawriter" under the **Database roles for iwss** heading. Save the settings.

Note: The IWSS machine name will appear under **IWSS > Users** after completing the steps above.

---

4. Refresh the IWSS management console

Troubleshooting Tips

- Issue: The management console displays the following error:

  ```
  JDBC-ODBC BRIDGE:[Microsoft][ODBC SQL Server Driver][SQL
  Server][Login failed for user 'DomainA\IWSSMachinename'.
  ```

  Solution: Check if "DomainA\IWSSMachinename$" along with "DomainA\machine_logon_user_name" (*UserA*) are included in the logins for SQL Server Enterprise under **Local > Database > Security > Logins**.

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

  Solution: Check the following:

  - Verify the user credential (*UserA*) for the SQL Server and the IWSS Server.
  - Make sure that the logon user (*UserA*) has the correct administrative rights on the 2 machines.

After Installing IWSS ICAP

Perform these post-install configuration steps if you have installed IWSS to use the ICAP HTTP handler.

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 server) 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.`" displays if you have not provided the required ICAP license key for NetCache.

4. Enter an ICAP license key:
   a. Click the **Setup** tab, and then click **System > Licenses** in the left menu. The **System Licenses** screen displays.
   b. Type your license under the **ICAP license** section.
   c. Click **Commit Changes**.
5. Select the **Service Farms** tab on the **ICAP 1.0** screen, and then click **New Service Farm** to add ICAP servers. Assign the service farm name in the **Service Farm Name** field.

- For response mode, select **RESPMOD_PRECACHE** in the **Vectoring Point** field
- For request mode, select **REQMOD_PRECACHE** in the **Vectoring Point** field

Select **Service Farm Enable**.

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

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

---

7. Under the **Consistency** field, choose **strong** from the drop-down menu and leave the **lbw Threshold** field empty.
8. Under the **Services** text box (for response mode), type:
   `icap://{ICAP-SERVER-IP}:1344/RESP-Service 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.
9. For multiple IWSS ICAP server services, type the additional entries in step 8. For example:

   For response mode,

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

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

   Click **Commit Changes**.

   For request mode,

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

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

   Click **Commit Changes**.

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

10. 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)" 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.

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

1. Select **Management**. Type the logon user name and password if prompted.
2. Click **ICAP** in the left menu, and then click the **ICAP Services** tab.
3. Click **New**. The **Add ICAP Service** screen displays.
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 displays.
6. Type or select the following information:
   a. The ICAP version number (that is, 1.0)
   b. The service URL, which includes the virus-scanning server host name or IP address, and the ICAP port number. The default ICAP port number is 1344.
      - Response mode:

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

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

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

---

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 displays. 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 displays, click **Grant this session**.

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

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 displays. Click **New** and select **Use ICAP Response Service**. The **Add ICAP Service Action** screen displays.

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:

i. Follow steps a to e in the previous procedure.

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

k. 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.

l. Click **Install Policies**.

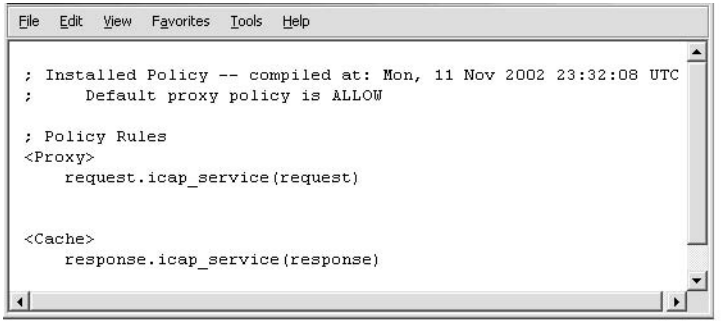


FIGURE 3-5 Configure both the request and response mode ICAP services. To check the current policy, go to the Policy screen, click the Policy Files tab, and then click Current Policy.

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, 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 displays.
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 displays.

6. Click **New** to add an ICAP service to the cluster. The **Add ICAP Cluster Entry** screen displays. 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 displays. 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 risk 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. To safeguard against this possibility, Trend Micro recommends flushing the cache immediately after installing IWSS ICAP. All new requests for Web content are 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 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**.

Enabling "X-Virus-ID" and "X-Infection-Found" Headers

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

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

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

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

For more details on the parameter values, see:

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

To enable the X-Virus-ID header:

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

Configuring Cisco Routers for WCCP Transparency

IWSS supports WCCP transparency when used in conjunction with a Cisco router. This section provides a brief introduction to configuring a Cisco router so that it works with IWSS.

IWSS supports the following WCCP features:

- WCCP version 2
- Generic Routing Encapsulation (GRE) HTTP and FTP packet redirection (L2-rewrite is not supported)
- Always uses service number 80
- HTTP (port 80) and FTP (port 21) are supported
- No password is supported

Note: Cisco IOS 12.2(23) through 12.3(9) has a known issue with WCCP connectivity. Trend Micro recommends not using these IOS versions.

Cisco 2600 Router Configuration Example

Consider the following network as an example:

- Two private network segments of 192.168.1.0/24 and 172.16.1.0/24
  - 192.168.1.0 is the network where clients reside
  - 172.16.1.0 has IWSS and presumably other servers, and has access to the Internet through a firewall
- The two networks are connected by a Cisco 2600 series router
- The router's FastEthernet 0/0 interface is connected to the 172.16.1.0 network with IP address 172.16.1.5 and FastEthernet 0/1 is connected to 192.168.1.0 with IP address 192.168.1.1
- 192.168.1.1 is the default gateway of the 192.168.1.0 network

- The IWSS server has IP address 172.16.1.101

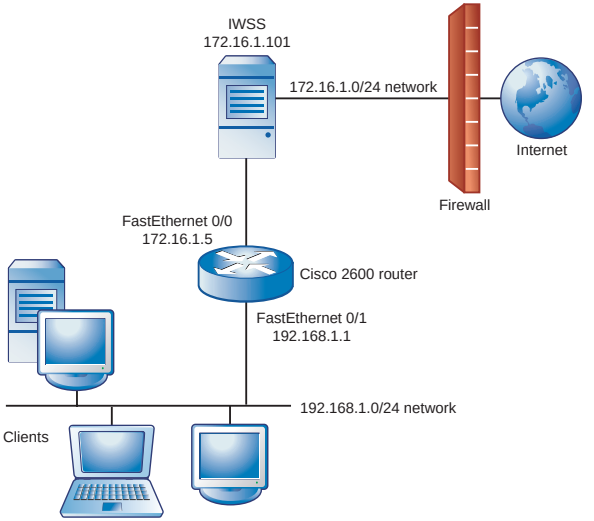


FIGURE 3-6 Sample network diagram

The Cisco router IOS command line configuration example is as follows:

```
hostname(config)# ip wccp 80 redirect-list 101 group-list 22

hostname(config)# access-list 22 permit 172.16.1.0 0.0.0.255
hostname(config)# access-list 101 permit tcp 192.168.1.0 0.0.0.255
any eq www
hostname(config)# access-list 101 permit tcp 192.168.1.0 0.0.0.255
any eq ftp

hostname(config)# interface FastEthernet0/0
hostname(config-if)# ip wccp 80 redirect out

hostname(config)# interface FastEthernet0/1
hostname(config-if)# ip wccp 80 redirect in
```

In this example, 80 is the WCCP service number. IWSS always uses service ID number 80. 101 and 22 represent the access control list number for clients and the WCCP proxy respectively, so these numbers can be arbitrary. WCCP version 2 is the default configuration in IOS 12.2 and 12.3, and GRE redirection is the only redirection option for the Cisco 2600 router, thus it's not required to configure the

WCCP version and redirection method. Note that there are other configuration possibilities.

Note: For more detailed options about IOS commands, refer to your Cisco router documentation.

IWSS Configuration

With the network described above, the IWSS configuration would be as follows:

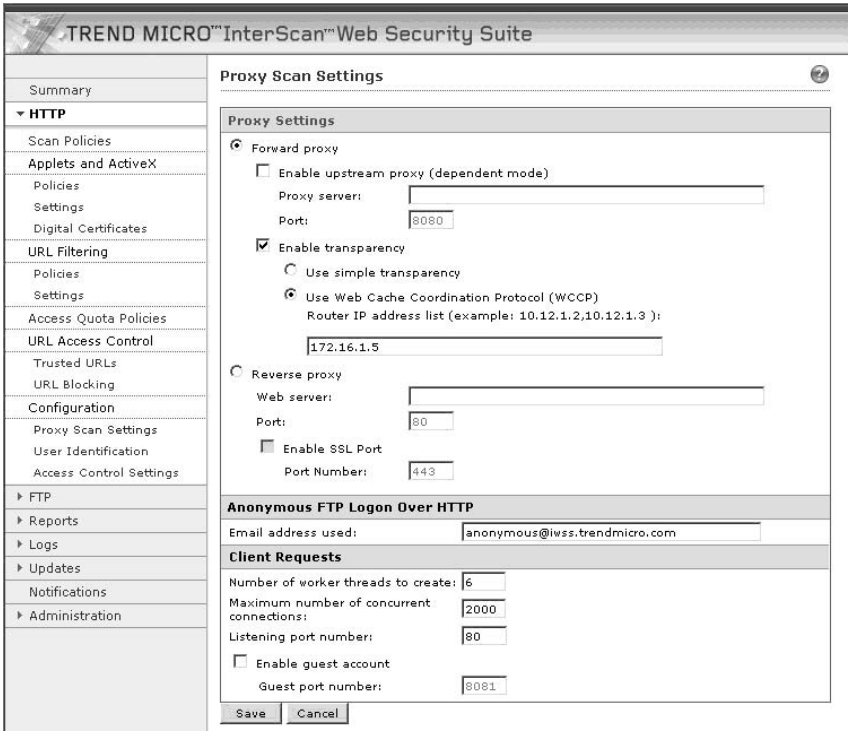


FIGURE 3-7 Proxy Scan settings for sample network using WCCP transparency

IWSS requires the GRE handler to receive WCCP GRE redirected packets correctly. The GRE handler is a device driver included in the IWSS package and is copied to the IWSS folder during installation. However, the GRE handler is not installed unless WCCP is chosen during installation. When WCCP is enabled via the management console, and the management console is opened from the machine where IWSS is installed without any proxy server in between, the management console automatically installs the GRE handler on the IWSS server. A window relating to the GRE handler's digital signature may display during installation—click **Yes** to continue the GRE handler installation.

Note: Depending on its signature signing status, the security window may indicate that the GRE handler does not have any digital signature.

If you try to connect to the IWSS management console from a remote machine, or if there is a proxy server between the browser and the IWSS server, the GRE handler will not be installed. Instead, a pop-up message displays advising you to install the GRE handler manually. In this case, the administrator must run the install_greh.exe command with the "-i" option from the Windows command line of the IWSS server. The installation program is copied to the <IWSS directory>\UtilBin\WCCP folder. The command to install the GRE handler from the default installation path is:

```
<Install_directory>\IWSS\UtilBin\WCCP\install_greh.exe –i
```

When installing the GRE handler from the command line, security messages are displayed in the same manner as installing through the management console. The install command can take the following parameters:

Parameter	Action
(No parameter)	Show usage
-i	Install
-u	Uninstall
-e	Enable
-d	Disable

When the GRE handler is sucessfully installed, the network connection's properties show the GRE Handler Driver is installed and enabled:

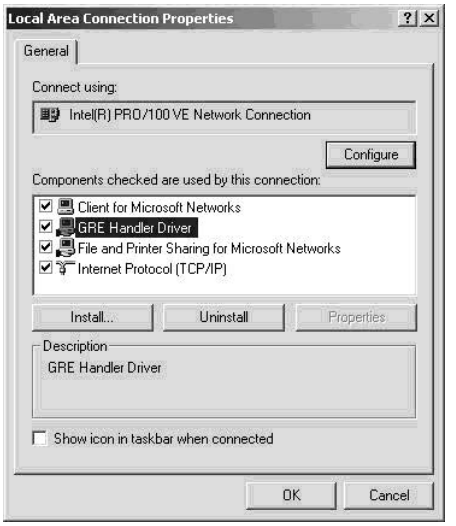


FIGURE 3-8 Network properties after installing GRE handler

When WCCP is no longer used and is disabled in the management console, the management console either automatically uninstalls the GRE handler or prompts you to uninstall it by running install_greh.exe –i. The GRE handler can also be removed from the Local Area Connection Properties dialog box by selecting **GRE Handler Driver** and clicking **Uninstall**. Installing and removing the GRE handler does not require rebooting the server. However, the network connection can be affected and some applications, for example, Internet Explorer, that show remote host directories are affected.

Testing IWSS

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

- Upload scanning
- FTP scanning

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

EICAR Test File

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

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

Obtaining the EICAR Test File

Download the EICAR test virus from the following URLs:

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

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

Alternatively, you can create your own EICAR test virus by typing or copying the following into a text file, and then naming the file “eicar.com”:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Note: Flush the cache in the cache server and local browser before testing. If either cache contains a copy of the test virus, it's possible an attempt to download the file would get the file from the cache, rather than getting it from the Internet, thus IWSS would not detect the file.

Upload Scanning

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

To test virus scanning of Web-based mail attachments:

1. Open the IWSS console and click **HTTP > Scan Policies** in the main menu. Clear **Enable virus scanning**, and then click **Save**.
2. Download the test virus from the following page:

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

FIGURE 3-9 This warning screen shows the detection of an EICAR test virus.

FTP Scanning

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

To test virus scanning of FTP traffic:

1. Download the test virus from the following page:

   `http://www.eicar.org/anti_virus_test_file.htm`
2. Access the FTP server through IWSS working as the FTP proxy.
   For example, assume the following IP addresses: IWSS FTP proxy server

(`10.2.10.2`), FTP server (`10.2.10.10`).
Open a command line prompt and type the following:

```
ftp 10.2.10.2
```

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

   ```
   put eicar_com.zip
   ```

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

FIGURE 3-10 This is a warning message that shows the detection of a virus in eicar_com.zip.

URL Blocking

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

Scan Settings in the main menu). Also, if you have not enabled transparency, client browsers must set their HTTP proxy to point to the IWSS server.

For more information about the HTTP topology, see *HTTP Proxy Topology* starting on page 8.

To test URL blocking:

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

FIGURE 3-11 A sample warning message for a blocked URL site.

Download Scanning

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

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

FIGURE 3-12 The above virus-warning screen displays if the system is set up properly.

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

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

URL Filtering

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

1. Click **HTTP > URL Filtering > Settings**. On the **URL Categories** tab, review the Web site categories that are classified as "Company Prohibited Sites."
2. Open the IWSS console and click **HTTP > URL Filtering > Policies** in the main menu. Select **Enable URL filtering** and click **Save**.
3. Click **URL Filtering Global Policy** and verify that "Company Prohibited Sites" are blocked during work and leisure time.

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

Java Applet and ActiveX Scanning

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

To test Java applet and ActiveX scanning:

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

Note: Blocking all Java applets and ActiveX controls may be too restrictive for your environment since it will prevent many legitimate Web sites from functioning properly. After testing, Trend Micro recommends going back to the **Applets and ActiveX Policy: Edit Global Policy** screen to change the settings back to the default or your own less-restrictive configuration.

About Hot Fixes, Patches, and Service Packs

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

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

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

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

`http://kb.trendmicro.com`

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

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

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

Appendix A

Technical Support and Troubleshooting

This chapter provides information to optimize your IWSS installation's performance and get further assistance with any technical support questions you may have.

Topics in this chapter include:

- Tuning performance through Windows TCP/IP settings and disabling optional product features
- Getting product updates from the Trend Micro Update Center
- Renewing the IWSS Maintenance Agreement
- Getting technical support
- Submitting suspicious files to Trend Micro for analysis
- Keeping abreast of the latest security threats through the Trend Micro Security Information Center

IWSS Performance Tuning

If experiencing issues with slow browsing performance, consider the following modifications to Windows TCP/IP settings and the IWSS remote rating service.

Windows Network Tuning

By default, Windows allows outbound network connections to bind to ephemeral ports in the range of 1025-5000, and keeps ports in the CLOSE_WAIT state for 240 seconds. While this is sufficient for most server software, it places a large bottleneck on proxy software like IWSS. For sustained traffic levels, the default Windows TCP/IP settings allow for a maximum of 3976/240 or about 16.5 requests per second. Persistent connections in HTTP 1.1 allow the actual traffic levels to exceed this hard limit, but for most deployments this will be problematic.

The ephemeral port range and TCP timed wait delay can be modified by changing entries in the Windows registry. The relevant entries are:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\MaxUserPort
```

and

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpTimedWaitDelay
```

Trend Micro recommends a value of 65530 for the *MaxUserPort*, and 60 for *TcpTimedWaitDelay*. This allows for a hard maximum sustained request rate of 1075 requests/second. After adding these entries, reboot the server for the settings to take effect.

Other Windows TCP/IP Settings

Any outgoing connection requires an ephemeral port to bind to, and is subject to the availability of those ports based on the *MaxUserPort* and *TcpTimedWaitDelay* settings. The recommended settings of 65530 and 60 provide for a maximum connection rate of 1075/second, but not all of these connections will be available to IWSS if the user/group name via proxy authorization (LDAP) identification method is in use, or if other proxy servers or network clients are running on the same server.

One common scenario is to chain IWSS to another proxy, such as Squid-NT or Microsoft ISA. When IWSS is chained to a Web proxy on the same server, each proxy will require an ephemeral port for every HTTP request, so using the Trend Micro recommended settings as the limit for sustained request rate will drop the maximum connection rate to 537 requests/second.

Using the user/group name via proxy authorization (LDAP) identification method also requires the IWSS server to connect to the directory server. IWSS supplies a cache mechanism for associating the source IP of incoming requests with a previously authenticated user, but if the cache is disabled, for example, if the incoming requests cannot be traced back to unique IPs due to an earlier Web proxy or router with NAT, then IWSS must authenticate each request with the directory server. In this worst case scenario, the sustained request rate limit will drop to 537/second for IWSS using LDAP on the server alone, or 358/second with IWSS and LDAP chained to a second Web proxy on the same server.

URL Filtering

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

Optionally, Trend Micro's remote rating service (RS) can be enabled. When enabled, IWSS will connect to this service via HTTP to request categorization for any URL that meets the following criteria:

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

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

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

The RS is disabled by default. To enable it, manually edit the file “urlfcIfx.ini” located in the “HTTP” folder of the IWSS installation folder. Set the value of the parameter [network]/no_web_access to “no” and restart the IWSS HTTP service.

LDAP Performance Tuning

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

LDAP Internal Caches

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

- User group membership cache: This cache can store the group membership information for several hundred users. By default, entries in this cache will be valid for 48 hours, or until the cache fills (at which point entries are replaced, starting with the oldest). The time to live (TTL) for entries in this cache can be configured via the setting “user_groups_central_cache_interval” in the [user-identification] section of intscan.ini configuration file.
- Client IP to User ID cache: This cache associates a client IP address with a user who recently authenticated from that same IP address. Any request originating from the same IP address as a previously authenticated request will be attributed to that user, provided the new request is issued within a configurable window of time (15 minutes by default for HTTP, 90 minutes for ICAP) from that authentication. The caveat is that client IP addresses seen by IWSS must be unique to a user within that time period, thus this cache is not useful in environments where there is a proxy server or source NAT between the clients and IWSS, or where DHCP frequently reassigns client IPs. To enable or disable

this cache, change the “enable_ip_user_cache” setting in the [user-identification] section of intscan.ini. To change the TTL of this cache, change the “ip_user_central_cache_interval” (unit is hours). For example, to create a TTL of 30 minutes, then enter “0.5”.

- User authentication cache: This avoids re-authenticating multiple HTTP requests passed over a persistent connection. When users pass the credential validation over a persistent connection, IWSS adds an entry (two important keys in one cache entry are the client’s IP address and the client’s username) in the user authentication cache so the subsequent requests over a keep-alive connection will not authenticate again. The client IP address and client’s username serve as two forward references, or links, to the “client IP to user ID cache” and “user group membership cache,” respectively. IWSS will thus still be able to retrieve the user’s connection information from both the IP-user and user-group caches.

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

Disable Verbose Logging When LDAP Enabled

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

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

Product Maintenance

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

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

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

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

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

FIGURE A-2 IWSS patches available on the Update Center

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

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 in to the account at the Trend Micro online registration Web site:

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

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

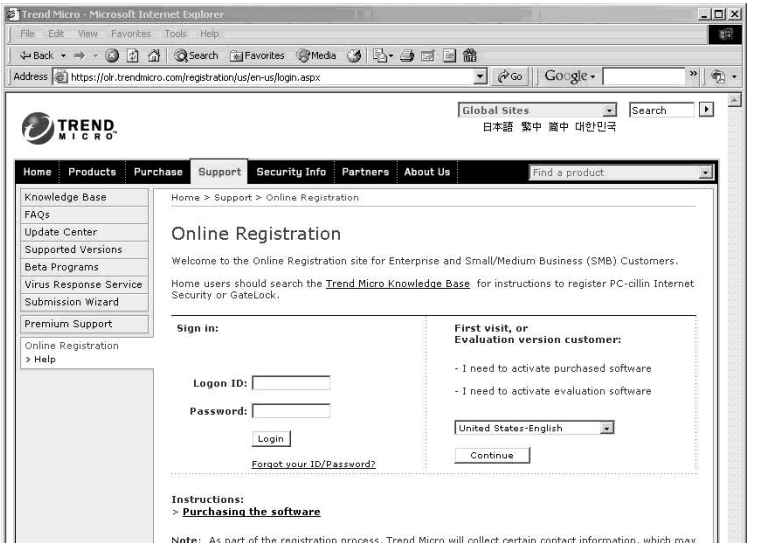


FIGURE A-3 Trend Micro Online Registration screen, used to enter or update your Registration Profile

Contacting Technical Support

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

`http://kb.trendmicro.com`

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

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

Follow the instructions for contacting support in your region.

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

`http://www.trendmicro.com`

`support@trendmicro.com`

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

General US phone and fax numbers follow:

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

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

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

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

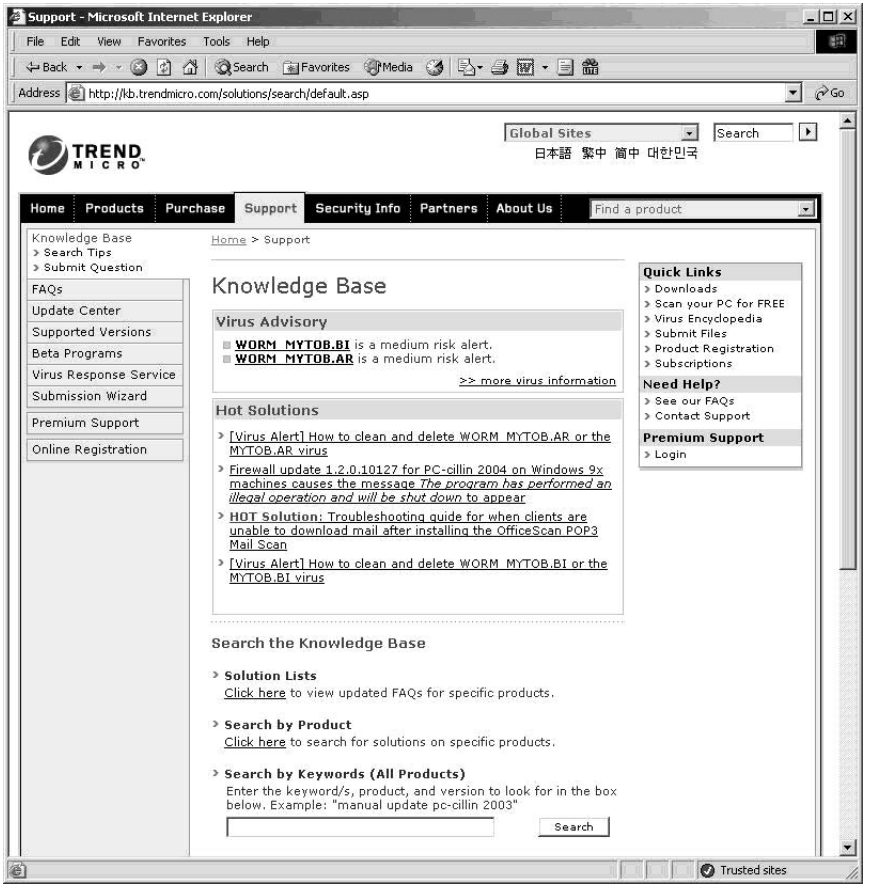


FIGURE A-4 Trend Micro Technical Support site.

TrendLabs

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

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

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

Knowledge Base

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

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

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

`http://kb.trendmicro.com`

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

Known Issues

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

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

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

`http://kb.trendmicro.com`

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

Sending Suspicious Code to Trend Micro

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

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

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

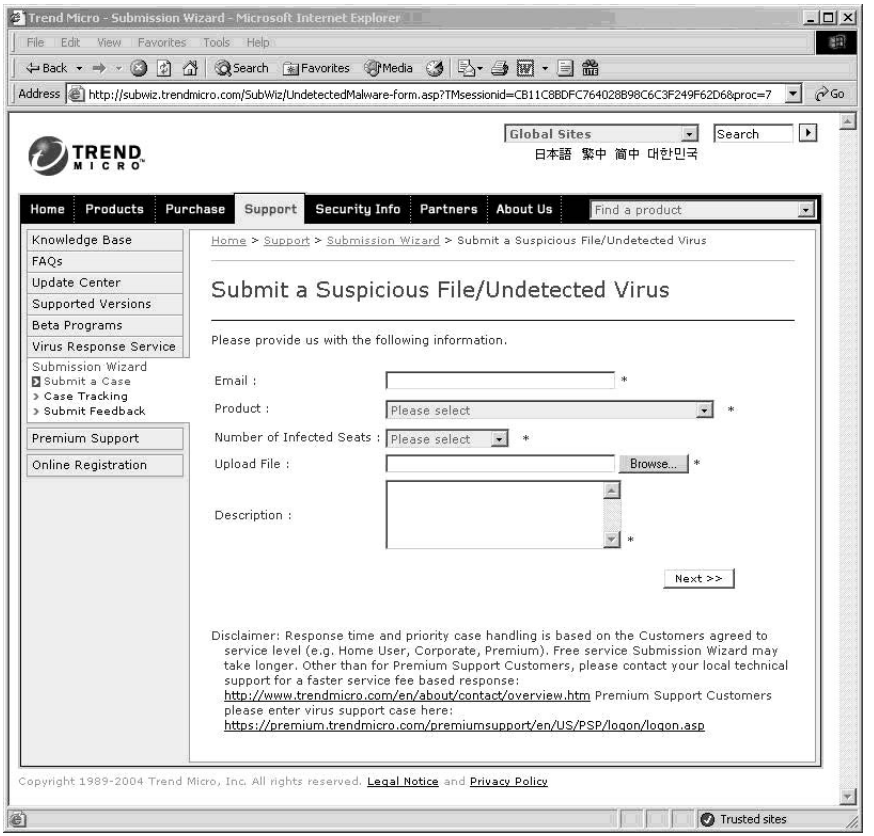


FIGURE A-5 Submission Wizard screen

You are prompted to supply the following information:

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

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

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

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

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

`virusresponse@trendmicro.com`

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

(877) TRENDAV, or 877-873-6328

Security Information Center

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

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

Visit the Security Information site to:

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

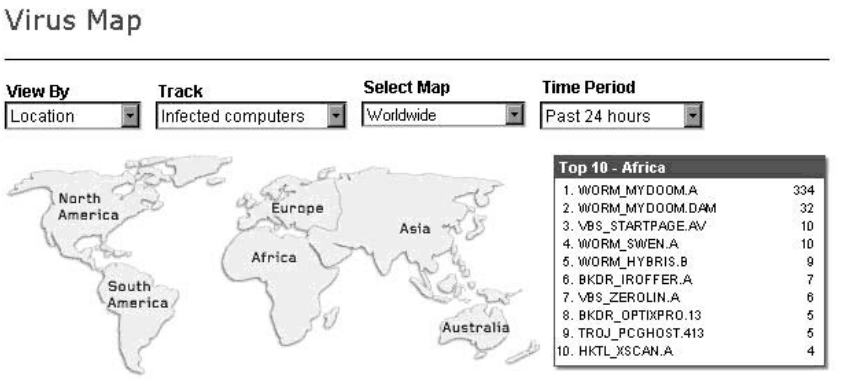


FIGURE A-6 Trend Micro World Virus Tracking Program virus map

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

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

To open Security Information:

1. Open the IWSS management console.

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

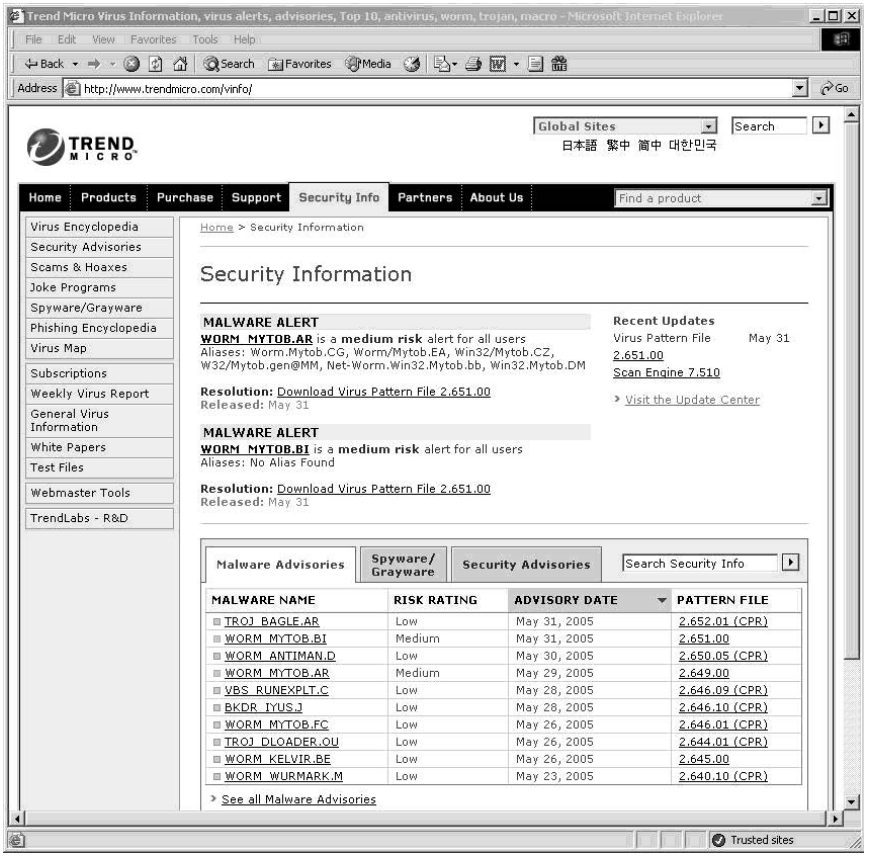


FIGURE A-7 Trend Micro Security Information screen.

About Trend Micro

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

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

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

`http://www.trendmicro.com`

Index

Q

R

S

T