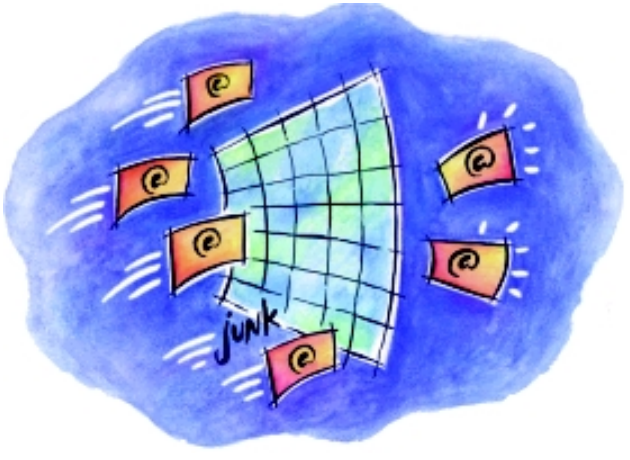
TREND MICRO InterScan 2 AppletTrap™



TREND MICRO™

Getting Started Guide

Document Part No. ATEM20869/11005
Release Date: August 2001

This manual, *Trend Micro InterScan AppletTrap Getting Started Guide*, is intended to introduce the main features of the software and install it into your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and online SolutionBank at Trend Micro's Web site.

http://solutionbank.antivirus.com/solutions/solutionsearch.asp

At Trend Micro, we are always seeking to improve our 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. You can also evaluate this documentation on the following site:

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

Table of Contents

Chapter 4: Getting Started

Chapter 5: Creating & Mapping Security Policies

Chapter 6: Configuring InterScan AppletTrap

Chapter 7: Maintaining AppletTrap and Contacting Technical Support

Chapter 1

Introducing InterScan™ AppletTrap™

InterScan AppletTrap is another in a long list of innovative Trend Micro products developed for the enterprise. InterScan AppletTrap blocks malicious Java applets, HTML scripts, as well as unsecured ActiveX controls at the Internet gateway—preventing them from infiltrating your network and performing malicious acts on client workstations.

In this chapter you will find:

- Product description
- How InterScan AppletTrap works
- Running with Trend VCS
- InterScan AppletTrap's benefits and capabilities

What is InterScan AppletTrap?

InterScan AppletTrap is now more than an HTTP proxy—it also includes support for Check Point's FireWall-1 CVP Interface. CVP stands for the Content Vectoring Protocol (CVP) Application Programming Interface (API) Specification. The CVP API is built upon the Open Platform for Security (OPSEC) foundation API.

InterScan AppletTrap employs a tiered technology approach that operates on both the Internet gateway server and on desktops. On the server, InterScan AppletTrap prefilters Java applets and ActiveX controls based on the certificates they carry, and uses updateable block lists to block known malicious Java applets and HTML scripts. Only the applets or scripts with recognized certificates that are not also included in the block lists are allowed to pass through the proxy server.

On client workstations, InterScan AppletTrap monitors the behavior of Java applets in real time and determines whether their behavior is malicious according to a preconfigured security policy. Malicious acts are handled accordingly and are reported back to the proxy server for inclusion in the block list. The next time InterScan AppletTrap encounters the same Java applet, it is blocked right at the entrance to the proxy server.

How Does InterScan AppletTrap Work?

Trend Micro InterScan AppletTrap detects and prevents Java applets, HTML scripts, and ActiveX controls from damaging or compromising computer system data. InterScan AppletTrap employs three levels of protection and distributes scanning tasks between the server and client workstations to spread the burden of malicious code detection across multiple computers.

On the server, (1) InterScan AppletTrap blocks ActiveX controls and Java applets with unrecognized certificates, and (2) uses updateable block lists to stop known malicious Java applets and HTML Scripts (JavaScript, VBScript, and/or all HTML Scripts). Only the applets and scripts with recognized signatures that are not included in the block lists are allowed to pass through AppletTrap.

On client workstations, (3) InterScan AppletTrap monitors the behavior of each Java applet in real time using a preconfigured security policy to determine whether or not its action is malicious. Any malicious applets detected are handled accordingly, and are reported back to AppletTrap for automatic inclusion in the block list. Figure 1-1 below illustrates how InterScan AppletTrap works.

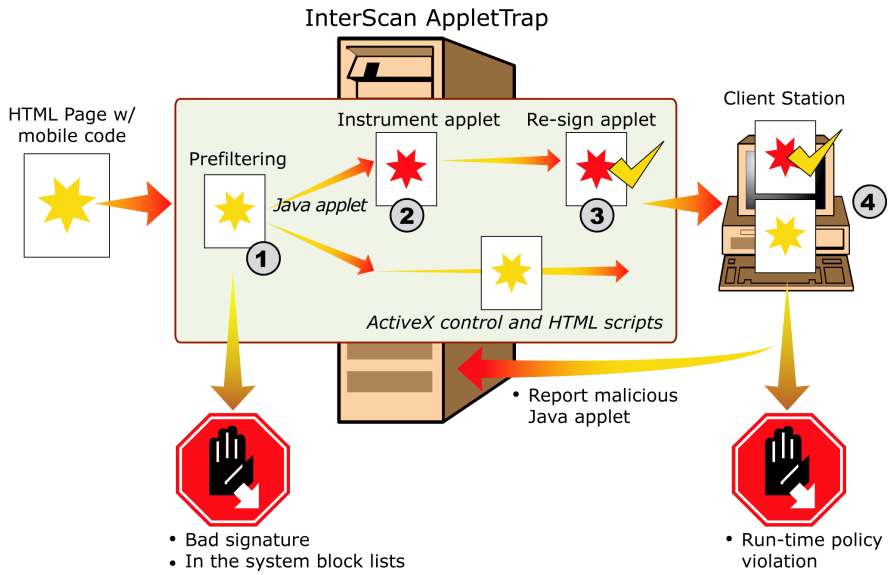


FIGURE 1-1. How InterScan AppletTrap works.

Step 1. Filters Java Applets, HTML Scripts & ActiveX Controls at the Server

As Java applets, JavaScript, VBScript, and ActiveX controls are downloaded to the proxy server, InterScan AppletTrap filters them according to the following criteria:

For Java applets...

InterScan AppletTrap filters Java applets based on the applet block lists and the certificates they carry, if certificate checking is enabled.

1. **InterScan AppletTrap compares the downloaded applets with the applet block lists**.

   InterScan AppletTrap keeps three updateable block lists for use in filtering known malicious applets. These lists include:

   - Downloadable hash list from Trend Micro containing the applets' hash codes; i.e., Message Digest (MD) 5 codes
   - User-configurable hash list
   - User-configurable list of specific Web sites that are known sources of malicious applets

   Any applets found in these lists are immediately discarded. In their place, the system creates a new applet that displays the following message when delivered to client workstations: **The applet has been identified to violate corporate security policy and is blocked**. In the case of access to a restricted site, the system creates a new HTML page containing the message: **The URL <URL address> is blocked by InterScan AppletTrap**. This new page is delivered to client workstations in place of the original page.

   InterScan AppletTrap dynamically updates the user-configurable hash list to include any malicious applets found on client workstations. You can also add applets to the user-configurable lists using the administrator console. Trend Micro's downloadable hash list is automatically updated during scheduled updates.

2. If certificate checking is enabled, InterScan AppletTrap checks the certificates applets carry. Those not signed, carrying an unrecognized certificate, or carrying a certificate that does not match what is contained in the file are blocked. They are then replaced with a new applet that displays the message: **This applet is not properly signed and is blocked**. If certificate checking is disabled, the system accepts all Java applets regardless of the certificates they carry.

InterScan AppletTrap keeps a database of recognized certificates, which is used in the filtering process. This database is automatically updated to include any unrecognized certificate the system encounters. You can delete entries from the database and enable or disable entries.

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

For ActiveX controls...

If ActiveX security is enabled, InterScan AppletTrap checks the certificates these objects carry and compares them with the Microsoft Internet Explorer certificate database. Controls not signed or carrying an unrecognized certificate are blocked. In their place, the system creates a new HTML page containing the message: **The URL <URL address> is blocked by InterScan AppletTrap**. This new page is then delivered to client workstations.

For URL blocking...

If URL blocking is enabled, InterScan AppletTrap restricts access to specific Web sites that are known sources of malicious HTML scripts. The system does this by comparing all client requests with the URL block list. Requests for URLs that are included in the list are blocked. In their place, InterScan AppletTrap creates a new HTML page containing the message: **The URL <URL> is blocked by InterScan AppletTrap**. This new page is then delivered to client workstations.

The URL block list contains the locations (i.e., URLs) of known malicious Java applets, JavaScript, VBScript, and/or all other HTML scripts. This list is user-configurable and can also be downloaded from Trend Micro through Internet updates.

For HTML script filtering...

If HTML script filtering is enabled, InterScan AppletTrap filters out all JavaScript, VBScript, and/or all HTML scripts according to the current configuration. Using HTML script filtering, the clients may access any URLs that are not on the block list. However, any scripts normally executed at that site will not be processed at the client. After filtering, the system delivers the text and accepted ActiveX controls to client workstations where they will be processed according to the security settings of the clients' Web browsers.

Step 2. Instruments Java Applets that Access System Resources

InterScan AppletTrap runs a quick check on how each Java applet will behave once delivered to client workstations, instrumenting those that will access system resources.

During instrumentation, InterScan AppletTrap inserts monitoring codes around suspicious instructions and then attaches the security policy assigned to the intended recipients. Depending on how InterScan AppletTrap is configured, this security policy may vary from one client to another based on the domain they belong to, or their IP addresses. InterScan AppletTrap supports creation of multiple policies that can be mapped to different groups of users in your network.

InterScan AppletTrap uses the inserted monitoring codes and the attached security policy to monitor the applet's behavior in real time and to determine whether or not this behavior is malicious.

Note: Instrumentation is a linear process that causes minimal overhead on the server. This process, however, renders the applets' certificates invalid due to code modification.

Step 3. Optionally Re-signs Instrumented Applets

If configured to do so, InterScan AppletTrap re-signs the instrumented applets using an imported "private key" before sending them to client workstations.

Since applets lose their original certificates during the instrumentation process (due to modifications to their original codes), you may want to use this feature to ensure that the clients' Web browsers will accept the instrumented applets. To accept, however, clients need to import the "public key" equivalent to your "private key" into to their browsers. Alternatively, the clients can simply disable certificate verification.

InterScan AppletTrap supports importation of a "private key" for use in the re-signing process. You can purchase this key from any of the well-known Certifying Authorities (CAs). Only one key is allowed to exist at any given time.

Note: Re-signing only applies to signed applets. If the system is configured to accept unsigned applets, these applets will bypass this process and will be delivered to client workstations immediately after instrumentation.

Step 4. Monitors the Behavior of the Instrumented Applets in Real Time

InterScan AppletTrap sends the instrumented applets to client workstations where they are again screened depending on the security settings of the Web browsers. Only when accepted and given access to resources will these instrumented applets be meaningful; i.e., InterScan AppletTrap and the browser should both agree before access is given to any of the system resources. For example, even if InterScan AppletTrap allows an applet to read files, if the client's Web browser is configured not to allow it, the applet will not be able to perform such an action.

Once given full access, the instrumented applet inserts monitoring codes that automatically execute when the instrumented instructions are run. Once invoked, these codes extract information about the resource(s) that will be used by the applet and determine whether this action is permitted by comparing it with the attached security policy. If the action is permitted, InterScan AppletTrap then allows the action to take place. Otherwise, InterScan AppletTrap takes the configured action. This action can be one of the following:

- Stop the current thread without notifying the user.
- Notify the user and give him/her the option to continue or terminate the thread created by the applet, or terminate the entire applet.

Note: An applet may create more than one thread.

- If enabled, automatically terminate the applet if the number of malicious offenses exceeds the configured tolerance.

Regardless of the action you select, InterScan AppletTrap reports back to the proxy server any malicious Java applets detected on client workstations for automatic inclusion in the user-configurable hash list. The next time the system encounters these applets, they will be blocked at the proxy server.

Running with Trend VCS

Trend Virus Control System (Trend VCS) is a centralized management console for coordinating, tracking, and maintaining the variety of antivirus software products installed on a network—regardless of platform or physical location.

InterScan AppletTrap is fully compatible with Trend VCS. You can configure multiple copies of InterScan AppletTrap using Trend VCS, and administer InterScan

AppletTrap along with your other Trend Micro antivirus products from a common Trend VCS console.

Other advantages of running InterScan AppletTrap with Trend VCS include:

- Aggregate log files for enterprise-wide virus statistics
- Centralized program file updates
- Uniform configuration standards
- Centralized configuration console
- Platform independence

To set up InterScan AppletTrap to work with Trend VCS, you need to register the server with the Trend VCS console. Once registered, you can access InterScan AppletTrap (and all other Trend VCS-registered programs) in the Trend VCS console via a Web browser by entering the URL and the Trend VCS password. From the Trend VCS console, InterScan AppletTrap can be administered in conjunction with all other antivirus products on the network.

Possible management schemes include:

- Have one administrator manage all antivirus programs, including InterScan AppletTrap
- Designate one administrator for all copies of InterScan AppletTrap installed on the LAN or WAN
- Assign InterScan AppletTrap to the local node administrator of the LAN where it resides

Of course, Trend VCS is not required to run InterScan AppletTrap—it can also be administered locally, from the machine where it was installed. But Trend VCS cannot set InterScan AppletTrap as a proxy to update its patterns, agents or programs. To update patterns, agents or programs for Trend VCS, you need to set its proxy to other proxy servers.

AppletTrap's Benefits & Capabilities

The following are the main benefits and capabilities of InterScan AppletTrap:

- **Better Performance and Stability.** The new version features a caching function that increases the performance throughput. This new version can handle more Web traffic with greater scanning accuracy.
- **Enhanced Security.** Central certification management at the Internet gateway creates a more secure e-business environment. Administrators can allow mobile codes from trusted partners to enter the enterprise with full permission, while still subjecting unknown codes to behavior monitoring.
- **Increased Scalability.** This version is highly scalable to support environments of over 5,000 users, or 500 concurrent users.
- **Check Point FireWall-1 support**. The FireWall-1 version has the added advantage that it is transparent to the end users.
- **Central certificate security management.** The Administrator can control the certification checking for Java applet/ActiveX security at the AppletTrap server.
- **Easy deployment**. Proxy server-based and only needs to be installed on one system.
- **Web-based updates.** Supports manual and scheduled updates via the Internet for easy and fast delivery of the latest block lists from Trend Micro's Web site to your system. Optionally uploads the local Java, URL, and ActiveX block lists to Trend Micro for potential inclusion in the Trend Micro block lists.
- **Load balancing**. Distributes the load between the proxy server or Firewall-1 server, and the clients, resulting in low overhead on each station.
- **Static filtering at the server**. Prefilters Java applets and ActiveX controls at the server based on the certificates they carry, and uses updateable block lists to filter known malicious Java applets, JavaScript, VBScript, and/or all HTMLScript.
- **Real-time code monitoring on client workstations for Java applets**. Employs Trend Micro's patented Instrumentation technology to monitor the behavior of Java applets on client workstations in real time. Any malicious act detected results in the termination of the current Java thread or the entire applet, depending on the configured action.
- **Dynamic block list updating**. Any malicious Java applets and ActiveX controls detected on client workstations are reported back to the proxy server for automatic inclusion in one of the system's block lists.

- **Customizable policies**. Supports customizable policies for controlling the behavior of applets on client workstations. These policies can be mapped to selected groups of users based on their IP addresses or domain.
- **Email notification**. Sends customizable email messages to the administrator and other designated recipients when URLs are blocked, malicious applets are found, and/or when the system certificate database gets updated.
- **Applet re-signing**. Optionally re-signs instrumented applets using an imported "private key" to ensure delivery to client workstations.
- **Comprehensive logs**. Provides comprehensive log files that record all key events as they occur.
- **Trend VCS-compatible**. Integrates with the Trend Virus Control System for consolidated operation with other antivirus programs on the network.

Chapter 2

Installing InterScan AppletTrap

In this chapter you will find:

- Minimum system requirements
- Preinstallation planning
- Step-by-step instructions for installing InterScan AppletTrap
- Verifying a Stand-alone installation
- Uninstalling InterScan AppletTrap
- Registering InterScan AppletTrap with Trend VCS
- License registration of InterScan AppletTrap

Minimum System Requirements

For the install machine...

InterScan AppletTrap can be installed on any server running Windows NT Server 4.0 (or above), Windows 2000, or Sun Sparc Solaris 2.5. In addition, the install machine must have at least:

For Windows NT and Windows 2000:

- 200MHz CPU (Intel Pentium, AMD, Cyrix, etc.)
- 128MB of RAM
- 128MB of swap space
- Cache space - default is 100MB
- Windows NT 4.0 with SP6 or Windows 2000 with SP1

For Solaris:

- 64MB of RAM
- 128MB of swap space
- Cache space - default is 100MB
- Solaris 2.6 or above
- Solaris patches for Java 2 SDK, Standard Edition v1.3

For the administrator console...

To access the administrator console, you need Internet Explorer 4.0 (or later) or Netscape 4.04 (or later). The browser used must also have its Java and JavaScript features enabled.

For chaining with other proxy servers...

InterScan AppletTrap can be chained with any standard proxy server such as Microsoft, Netscape, Apache, and CERN.

For running with a Check Point FireWall-1 server...

Check Point FireWall-1, CVP edition—FireWall-1 3.0b (Build 3064 or above) or FireWall-1 4.x

For clients...

A Java-enabled Web browser such as Netscape Communicator 4.04 (or later) or Microsoft Internet Explorer 3.02 (or later).

Installation Overview

Installing InterScan AppletTrap on your network is comprised of three major steps:

1. Preparing the client workstations and existing proxy servers for installation.
2. Installing the InterScan AppletTrap program files.
3. Incorporating InterScan AppletTrap into your network configuration. This step is described in Chapter 3, "Incorporating AppletTrap into the Network".

InterScan AppletTrap's installation is simple and only takes a few minutes. Prior to installation, you need to locate the serial number on the front cover of this Getting Started Guide or obtain one from a sales representative at:

```
sales@trendmicro.com
```

Without this information, Setup installs the 30-day trial version.

Preinstallation Planning

InterScan AppletTrap can be configured to function as a stand-alone proxy server, to be chained with any standard proxy server, or to function as a plug-in to a FireWall-1 server. You can install AppletTrap on:

- A dedicated server (Standard or FireWall-1 version)
- The same machine as an existing proxy server (Standard version)
- The same machine as an existing FireWall-1 server (FireWall-1 version)

Why install on a dedicated server?

- Less resource intensive — running two proxy services, or AppletTrap and a firewall, on the same machine can compromise performance
- Avoids service port conflicts

In this topology, if InterScan AppletTrap is the only proxy server on the network, you need to configure the client browsers to use InterScan AppletTrap as the proxy server.

If, however, you have no other choice but to have all proxies on one machine, ensure that no two services bind to the same service port. By default, InterScan AppletTrap binds to service port 8080. If this setting conflicts with another, modify it (as described later in this chapter) or the one it conflicts with.

For a list of ports already in use by the different services in your system, go to the Windows NT install directory (e.g., C:\Winnt\system32\drivers\etc\) and open the file **Services** using a text editor program.

Why install on an existing proxy server?

- Does not require another server
- Does not require configuration changes on client browsers

In this topology, configuration changes on clients' browsers are not necessary if InterScan AppletTrap is not placed closest to clients. However, you need to make sure no two services bind to the same port on the same server. Also, note that putting two proxy services on the same machine can compromise performance.

Note: In a multi-proxy scenario where another proxy server exists between the InterScan AppletTrap and the Internet, you need to ensure that the server does not block any incoming Java applets, JavaScript, and ActiveX controls. Leave all mobile code processing to the InterScan AppletTrap proxy server.

Why install on an existing FireWall-1 server?

- Does not require another server
- Does not require configuration changes on client browsers

In this topology, configuration changes on clients' browsers are not necessary. However, note that putting AppletTrap on the same machine as FireWall-1 can compromise performance.

Incorporating InterScan AppletTrap into your network

Generally speaking, it is best to install AppletTrap on a server that is inside the firewall, if any. It should also be placed "in front" of the server or proxy server it will complement. In other words, after a firewall, AppletTrap should be the first in line to receive the network HTTP traffic. You may need to modify your firewall configuration (IP and/or port) so it routes traffic to AppletTrap.

The AppletTrap server receives inbound and outbound Internet traffic as it crosses the gateway, checks for malicious code, and then sends the traffic on for delivery as usual.

Running as a Stand-alone Proxy

Incorporating the InterScan AppletTrap proxy server into your network is simple and only requires minimal configuration. As a stand-alone proxy server, you only need to configure your clients' Web browsers to use the InterScan AppletTrap proxy server. By default, InterScan AppletTrap runs as a stand-alone proxy server.

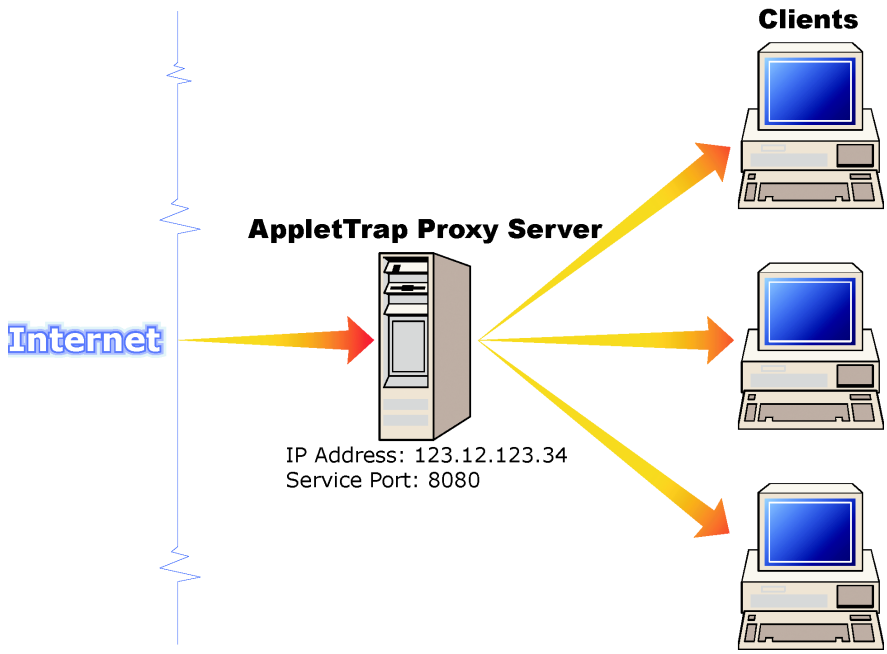


FIGURE 2-1. InterScan AppletTrap as a stand-alone proxy server.

Chaining InterScan AppletTrap with Existing Proxy Servers

As a stand-alone server, InterScan AppletTrap supports methods for retrieving HTTP and FTP resources. Caching, however, is not supported.

For better performance, you can chain the InterScan AppletTrap proxy server with another HTTP proxy server that provides the caching functionality. This caching proxy server must be placed closer to the client workstations than the InterScan AppletTrap proxy server. This configuration maximizes cache usage and minimizes repeated instrumentation of the same applet.

If another proxy server exists between the InterScan AppletTrap proxy server and the Internet, you need to ensure that the server does not block any incoming Java applets, JavaScript, and ActiveX controls, if it provides such functionality. Leave all mobile code processing to the InterScan AppletTrap proxy server.

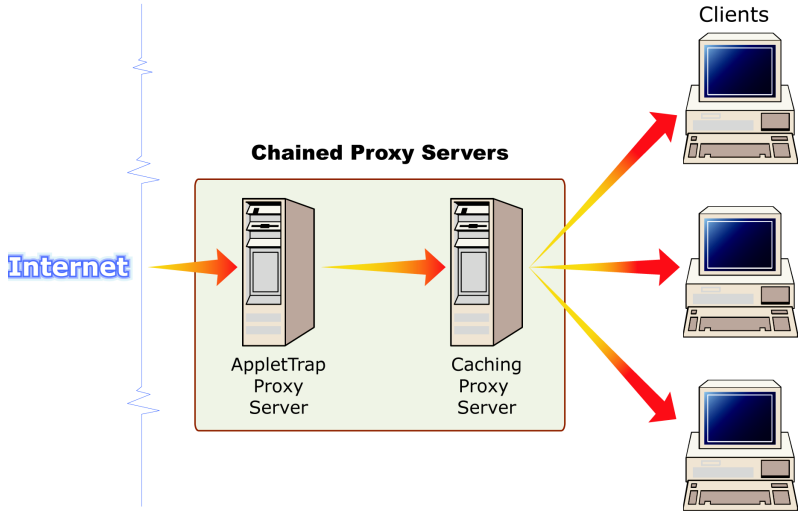


FIGURE 2-2. Sample network topology with chained proxy servers.

Installing InterScan AppletTrap Connected to an Existing Check Point FireWall-1

For better performance, you can install the InterScan AppletTrap on a dedicated proxy server and connect to a Check Point FireWall-1 server.

FireWall-1 operates at the packet level, distributing the individual packets it receives on the basis of protocol type and the policies that are defined in the FireWall-1 rule base. In order for AppletTrap to receive these packets from FireWall-1, **Network, Server, Service,** and **Resource** objects representing the AppletTrap server and AppletTrap services must be defined and added to the rule base.

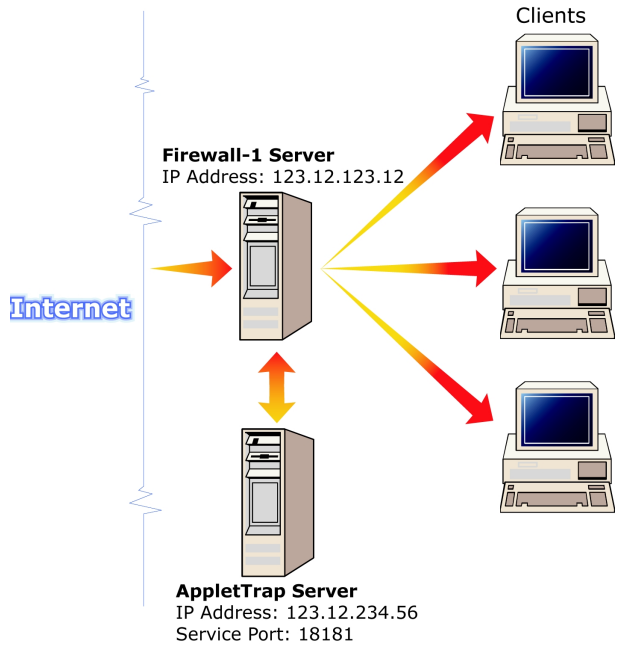


FIGURE 2-3. Sample network topology with AppletTrap on a dedicated server, connected to a FireWall-1 server.

1. Configure FireWall-1 to use InterScan AppletTrap as a CVP server. These steps are fully described in Chapter 3, "Incorporating InterScan AppletTrap into the Network".

   a. AppletTrap: Setting the AppletTrap Service Port

   b. FireWall-1: Creating a Network Object

   c. FireWall-1: Creating a Server Object

   d. FireWall-1: Creating a Resource Object

   e. FireWall-1: Adding a Rule to the Rule Base

   f. FireWall-1: Installing the Rule

   g. Setting up Check Point's Authentication for AppletTrap

2. There is no need to change the clients' browser configuration since they are still using the same machine as before.

Installation Steps

Step 1: Preparing the system for installation

To start with a clean slate, you need to clear the cache on both your clients and any existing proxy servers.

The procedure for clearing the cache on client workstations varies according to the browser used. The same is true for proxy servers. For information on clearing cache on proxy servers, please refer to their documentation. For information on clearing the clients' cache, see the following sections. If you are using a different browser than the ones mentioned below, please refer to its manual for information.

Clearing the Cache on Netscape Communicator:

1. Open Netscape Communicator and go to **Edit** >**Preferences.**
2. Click on **Advanced** in the left pane and choose **Cache**.
3. Click **Clear Memory Cache**, then **Clear Disk Cache**. Select **OK** on the confirmation screens and **OK** again to close the window.

Clearing the Cache on Internet Explorer:

1. Open Internet Explorer and go to **Tools > Internet Options...**.

   -or-

   right-click on the Internet Explorer icon on your desktop and choose **Properties**.
2. Select the **General** tab.
3. Under **Temporary Internet files**, click **Delete Files**, then **OK**.
4. Click **OK** to close the window.

Step 2: Installing InterScan AppletTrap

To install the Standard version on a Windows Server...

To install InterScan AppletTrap, you must be logged on to the system using a Windows administrator account. Create a local user, then provide both the local user and administrator with the advanced user rights to "Act as part of the operating system" and "Log on as service". If you are installing AppletTrap for the first time, please refer first to the latest ReadMe text, which can be obtained from the following site, before proceeding to the installation procedure:

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

1. If you have the Trend Micro Enterprise Solution CD, run **go.exe** by inserting the CD into the CD-ROM drive or by running the program from the Start menu, select the appropriate language. Click **Install** and then select **InterScan AppletTrap** from the list at the right. Then click **Install**.

   -or-

   If you have downloaded InterScan AppletTrap from Trend Micro's Web site, unzip the program and double-click **Setup.exe**.

2. Click **Next** on the Welcome screen and **Yes** to accept the License Agreement.
3. Select **Standard version**, click **Next**.
4. In the User Information dialog box, enter the requested information and then click **Next**. A 30-day trial version is installed if you do not enter a serial number.
5. In the Choose Destination Location dialog box, accept the default install directory, or specify a different location using the **Browse** button. Click **Next** to continue.
6. Click **Next** in the Select Program Folder dialog box, then select the program folder on the next screen.
7. In the Service Account dialog box, assign an account for the InterScan AppletTrap service. Make sure this is a Windows Administrator account with the advanced user rights to "Act as part of the operating system" and "Log on as a service".

   Take note of the account you specify here, you will need to log on using this same account when you modify the certificate database of Internet Explorer from the administrator console.

8. Click **Next** to start copying the InterScan AppletTrap files to the selected destination.
9. Click **Finish** on the next screen to complete installation.

Installing the Standard version on a Solaris Server

You need to have the root permission to install InterScan AppletTrap on a Solaris server.

1. Copy the **atxxsolaris.tar.gz** file to a \temp directory. "xx" denotes the program version, thus **at25solaris.tar.gz** is the setup program for InterScan AppletTrap 2.5.
2. Use the following commands to extract the archive:

```
#gzip -d at25solaris.tar.gz
#tar xvf at25solaris.tar
```

3. Run the install script:

```
#./install
```

4. When prompted, agree to the License Agreement and enter your name, your company's name and a serial number. Press **Enter** if you want to install a trial version, then confirm the information just entered.
5. After installation completes, the program is located in the `/opt/trend/InterScan_AppletTrap` directory.

Installing the Check Point FireWall-1 version

To install InterScan AppletTrap, you must be logged on to the system using a Windows administrator account. Create a local user, then provide both the local user and administrator with the advanced user rights to "Act as part of the operating system" and "Log on as service". If you are installing AppletTrap for the first time, please refer first to the latest ReadMe text, which can be obtained from the following site, before proceeding to the installation procedure:

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

1. Insert the Trend Micro Enterprise Solution CD, invoke **go.exe** by running the program from the **Start** menu, and then select the appropriate language. Click **Install** and then select **InterScan AppletTrap** from the list at the right. Then click **Install**.

-or-

If you have downloaded InterScan AppletTrap from Trend Micro's Web site, unzip the program and double-click **Setup.exe**.

2. Click **Next** on the Welcome screen and **Yes** to accept the License Agreement.
3. Select **CVP edition for FireWall-1**, click **Next**.
4. In the User Information dialog box, enter the requested information and then click **Next**. A 30-day trial version is installed if you do not fill in a serial number.
5. In the Choose Destination dialog box, accept the default install directory, or specify a different location using the **Browse** button. Click **Next** to continue.
6. Select the program folder on the next screen, then click **Next**.
7. In the Service Account dialog box, assign an account for the InterScan AppletTrap service. Make sure this account is a Windows Administrator account with the advanced user rights to "Act as part of the operating system" and "Log on as a service".

   Take note of the account you specify here, you will need to log on using this same account when you modify the certificate database of Internet Explorer from the administrator console.
8. Click **Next** to start copying the InterScan AppletTrap files to the selected destination.
9. Enter the FireWall-1 CVP port number that AppletTrap will run on (the default is 18181), then click **Next**.
10. Click **Finish** on the next screen to complete installation.

Step 3: Accessing the Administrator Console

InterScan AppletTrap comes with a web-based administrator console for centrally administering the InterScan AppletTrap proxy servers on the network. This console requires at least Internet Explorer 4.0 or Netscape 4.04. In addition, the Web browser used must have its Java and JavaScript functions enabled to take advantage of all the product features.

Note: To prevent connection failures that may occur during system configuration, make sure the Web browser accessing the administrator console is not chained to any InterScan AppletTrap proxy server.

To access the administrator console...

1. If you are accessing the console locally, select **Programs > InterScan AppletTrap > AppletTrap Administration** from the Windows **Start** menu.

   If you are accessing the console from a remote site, open your Web browser and connect to the following URL:

   http://<server>:<configport>/

   where **<server>** is the IP address or host name of the InterScan AppletTrap proxy server, and **<configport>** is the remote management port. By default, this value is 2222. For example,

   http://us-philr:2222/

2. On the logon screen, enter **admin** in the User name text box and the current system password. The default system password is **trend**. Both values are case-sensitive.
3. Click **OK**. The Trend Micro InterScan AppletTrap main screen appears.

Step 4: Resolving conflicts in service port usage

In the event that the default service port of InterScan AppletTrap conflicts with another service on the install machine, bind InterScan AppletTrap or the service it conflicts with to another port. By default, InterScan AppletTrap binds to port 8080 in the Standard version and port 18181 in the FireWall-1 version.

To bind InterScan AppletTrap to another service port,

1. From the left pane of the Trend Micro InterScan AppletTrap main screen, select **Server Administration**. The Server Administration page appears on the right pane.
2. On the Server Administration page, enter an unused service port at **Bind service port at** (for Standard version), or **CVP server port (**for FireWall-1 version).
3. Scroll down and click **Apply**.

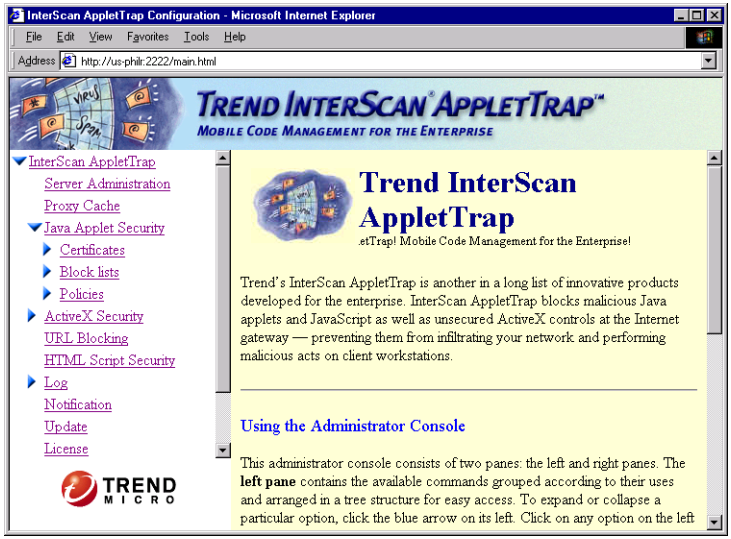


FIGURE 2-4. The InterScan AppletTrap main screen (Standard version).

Verifying a Stand-alone Installation

If you installed AppletTrap on a dedicated server, you can perform a simple test to make sure that it is installed and configured correctly. InterScan AppletTrap is up and running by the time the installation has finished. You can click on **InterScan AppletTrap** on the left pane to verify that AppletTrap is running.

The example given below is a test of the URL blocking feature.

1. On the administrator console, click on **URL Blocking** in the left pane. The URL Blocking page appears on the right.
2. Make sure **Enable this block list** is checked. Click **Add URL** and enter a URL in the JavaScript Prompt popped up accordingly. Click **OK** at the prompt, then **Apply** on the URL Blocking page.
3. On a browser that has InterScan AppletTrap as the proxy server, type that URL in the address text box.

You should see an error message on your browser: **The URL <the blocked URL:80> is blocked by InterScan AppletTrap**, indicating that the installation was successful.

Note: On Windows NT, when concurrent requests exceed the backlog of system winsock setting, a connection failure may occur. In order to resolve this issue, the Windows registry should be modified. Please find the steps to be followed in modifying some keys in the Windows registry from Trend Micro's online Knowledge Database called SolutionBank or contact Technical support.

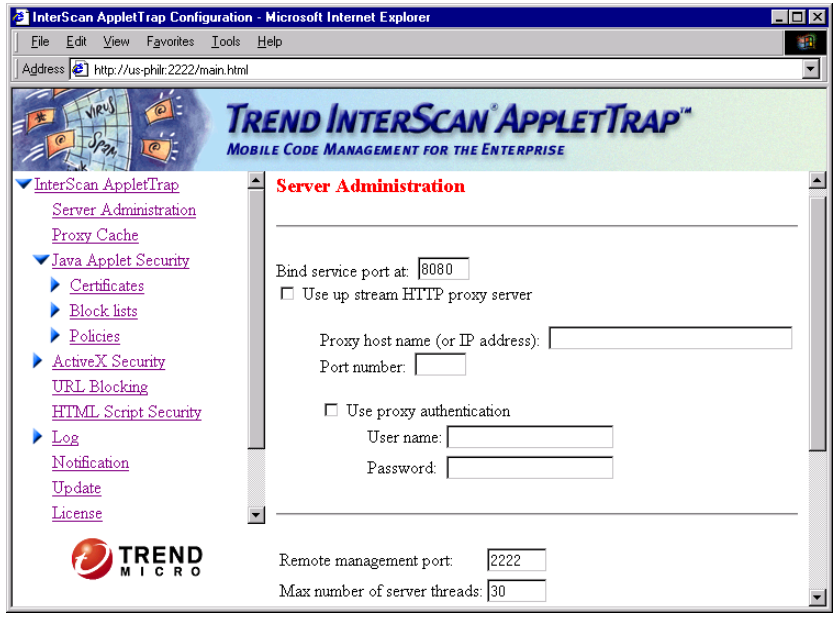


FIGURE 2-5. Server Administration page (Standard version) for specifying the configuration of the InterScan AppletTrap proxy server.

Uninstalling InterScan AppletTrap

Before installing a new version of InterScan AppletTrap on your system, first remove the older version by following the steps below. The uninstall program will remind you if the InterScan AppletTrap service is still running. Stop the service to continue the uninstallation.

Uninstalling from a Windows Server

1. Select **Programs > Trend InterScan AppletTrap > Uninstall AppletTrap** from the Windows **Start** menu.
2. Click **Yes** on the Confirm File Deletion screen.

Uninstalling from a Solaris Server

You need to have root permission to uninstall InterScan AppletTrap from a Solaris server.

1. Change to the directory:

```
cd /opt/trend/InterScan_AppletTrap/
```

2. Run the uninstall script:

```
#./uninstall
```

If you are not reinstalling, do not forget to reconfigure the clients and proxy server chain back to the configuration they were in before InterScan AppletTrap was installed.

Disable the use of proxy server in client browsers if InterScan AppletTrap was installed as a stand-alone proxy server. If it was incorporated into a multi-proxy environment, you should modify the existing proxy configuration (which used to point to InterScan AppletTrap) to use another valid proxy server. Please refer to the manufacturer's manuals of your existing proxy servers for details regarding proxy configuration.

Registering InterScan AppletTrap with Trend VCS

InterScan AppletTrap comes fully compatible with the Trend Virus Control System. This means that, in addition to its administrator console, you can also administer InterScan AppletTrap from a Trend VCS console.

To set up InterScan AppletTrap to work with Trend VCS, you need to register the server with the Trend VCS console.

To register InterScan AppletTrap with Trend VCS,

1. From the left pane, select **TVCS Registration**.
2. Under **TVCS Server**, enter the IP address (or host name) of the TVCS server, its server port, and site name in the provided text boxes.

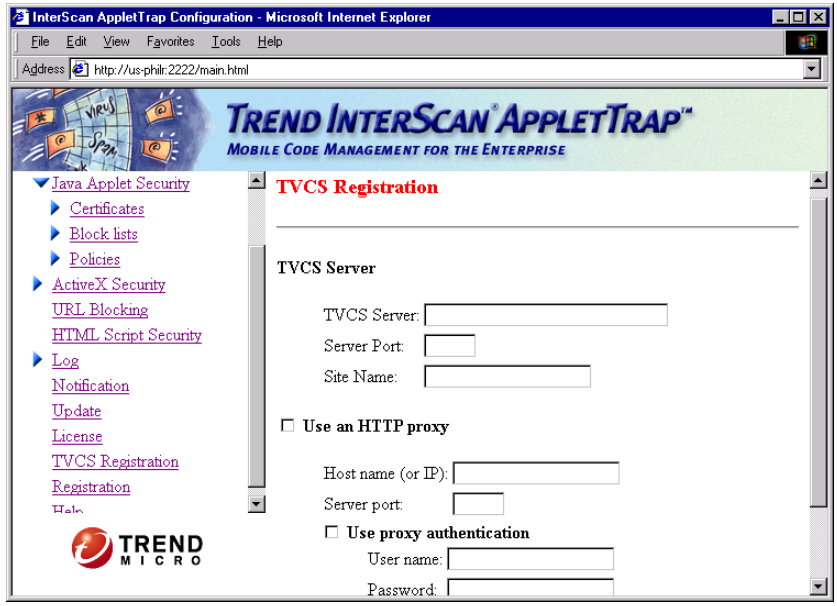


FIGURE 2-6. You need to register InterScan AppletTrap with Trend VCS to enable management from the Trend VCS console.

3. If you need to pass through a proxy server to reach the TVCS server, check **Use an HTTP proxy** and then enter the requested information.
   - Enter the host name or IP address of the HTTP proxy in the Host name (or IP) text box.
   - Specify the server's service port in **Server port**.
   - Check **Use proxy authentication** and then specify the username and password if required to log on to the proxy.
4. Scroll down and click **Register**.

License Registration of InterScan AppletTrap

InterScan AppletTrap allows you to test run the program by installing its 30-day trial version. This version is fully functional and can be installed without entering a serial number. After 30 days, however, most program features will no longer function.

To upgrade your 30-day trial version, you just need to enter the product serial number. You can get this information from the front cover of this Getting Started Guide, or from a Trend Micro sales representative at the following email address:

```
sales@trendmicro.com
```

You do not need to reinstall InterScan AppletTrap to upgrade to the full version.

To remove the 30-day trial limit...

1. From the left pane, select **License**.
2. Enter the product serial number in the provided text box.
3. Click **Register**.

Chapter 3

Incorporating AppletTrap into the Network

In this chapter you will find procedural steps for incorporating InterScan AppletTrap into the network, including:

- Clearing cache on client browsers/proxy servers
- Configuring AppletTrap to run as a Stand-alone server (Standard version)
- Configuring AppletTrap to run on a network with existing proxy servers (Standard version)
- Configuring AppletTrap to run with FireWall-1 server (FireWall-1 version)

Clearing Cache on Client Browsers/Proxy Servers

To start with a clean slate, clear the cache on both your clients and any existing proxy servers. This prevents potential malicious applets from being retrieved from local cache (which is not scanned by InterScan AppletTrap).

Note: If you are using the Standard version of AppletTrap, to save configuration time you may want to execute this step at the same time that you change your client browsers to point to the AppletTrap server.

For instructions on clearing the cache, see the section "Installation Steps, Step 1: Preparing the system for installation" in Chapter 2, "Installing InterScan AppletTrap".

Configuring InterScan AppletTrap to Run as a Stand-alone Server (Standard version)

A. Configure InterScan AppletTrap as a Stand-alone proxy server

1. From the left pane, select **Server Administration**. The Server Administration page appears on the right pane.
2. Clear the **Use up stream HTTP proxy server** checkbox.
3. Click **Apply**.

B. Configure the clients' Web browsers to use the InterScan AppletTrap proxy server

For Netscape Communicator:

1. Open Netscape Communicator and select **Preferences** from the **Edit** menu.
2. From the **Category** group box at the left, expand **Advanced**.
3. Select **Proxies** to display the Proxies page at the right.
4. Check **Manual proxy configuration** and then click the **View** button.
5. Enter the InterScan AppletTrap IP address and service port in the **HTTP** and **Port** text boxes, respectively.

6. Click **OK** twice to apply the new configuration.
7. Restart the browser.

For Internet Explorer:

1. Open Internet Explorer and select **Internet Options** from the **View** menu.
2. Select the **Connections** tab and click **LAN Settings**, and enable **Use a proxy server**. Then, click **Advanced**.
3. Enter the InterScan AppletTrap IP address and service port in the HTTP and Port text boxes, respectively.
4. Click **OK** twice to apply the new configuration.
5. Restart the browser.

For multiple proxy server configuration, the procedure varies depending on how you want to position these servers in the chain. As mentioned earlier, it is best to position the InterScan AppletTrap proxy server closest to the Internet. Caching proxy servers should be placed closer to client workstations to maximize cache usage and to minimize repeated instrumentation of the same applet.

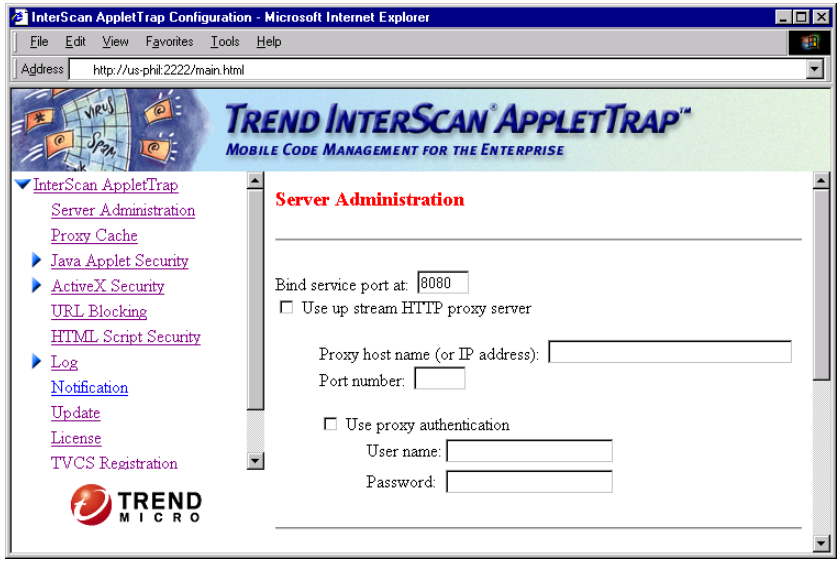


FIGURE 3-1. Configuring InterScan AppletTrap as a stand-alone proxy server.

Configuring InterScan AppletTrap to Run with an Existing Proxy Server

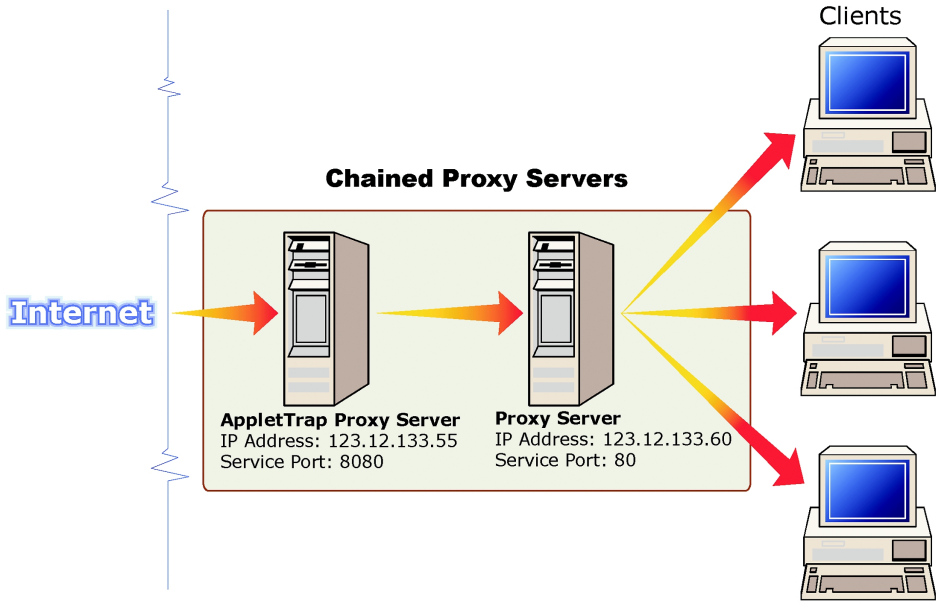


FIGURE 3-2. Using InterScan AppletTrap with an existing proxy server.

A. Configure InterScan AppletTrap Proxy Server

1. From the left pane, select **Server Administration**. The Server Administration page appears on the right pane.
2. Check the **Use up stream HTTP proxy server** checkbox and then enter the IP address (or server name) and service port of the Proxy Server in the **Proxy host name (or IP address)** and **Port number** text boxes, respectively. The default value for the service port is 8080.

   For proxy authentication, enable **Use proxy authentication** and enter the **User name** and **Password** for verifications.
3. Scroll down and click **Apply**.

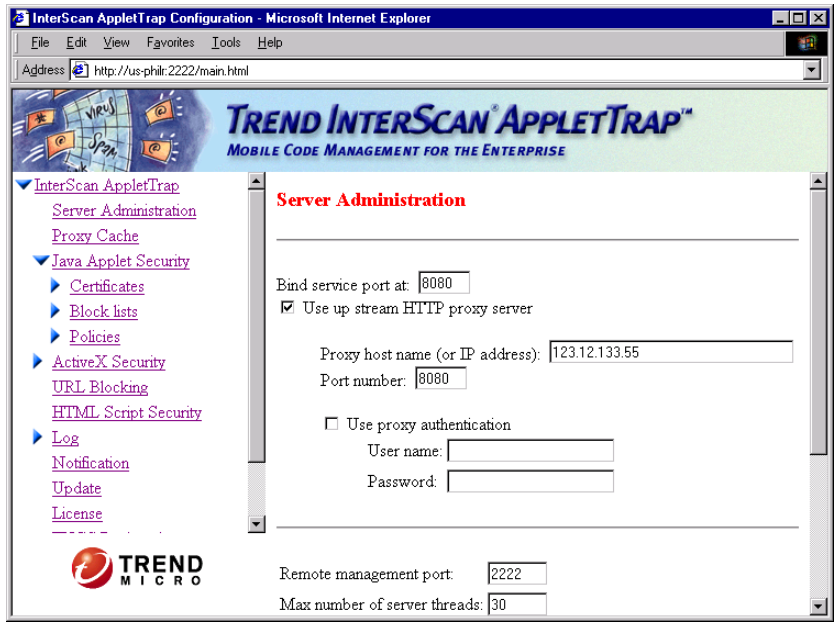


FIGURE 3-3. Configuring InterScan AppletTrap to use up stream HTTP proxy server.

B. Configure the clients' Web browsers to use Proxy Server

Using our example, you need to configure your clients' Web browsers to use Proxy Server at IP address 123.12.133.60 and service port 80. Please refer to the previous section for information on how to do this.

Configuring InterScan AppletTrap to Run with FireWall-1

In the following sections, the procedure to configure InterScan AppletTrap to work as a plug-in to your FireWall-1 server is described. The steps are the same either running AppletTrap as a stand-alone server or running AppletTrap on the FireWall-1 server.

A. AppletTrap: Setting the AppletTrap Service Port

The **CVP Service Port** used by AppletTrap is typically set during installation. The default is *18181* for AppletTrap; however, any free port can be used.

To change the **CVP Service Port** used by AppletTrap,

1. Open the AppletTrap configuration in a Web browser and click **Server Administration** in the left window pane.
2. In the **CVP server port** field, enter the port number that you will later use when editing the FW1-CVP **Service Object** in FireWall-1.

After installing AppletTrap onto the machine(s) where it will reside, connect to the FireWall-1 machine and start the configuration interface. Each of the four FireWall-1 tasks is described below.

B. FireWall -1: Creating a Network Object

1. In the FireWall-1 configuration page, click **Manage > Network Objects**.
2. Click **New**, then choose **Workstation** (or choose an existing Network object representing the AppletTrap machine).
3. In the **General** tab, enter the name of the machine where AppletTrap is installed in the **Name:** field. For example,

   `US-AppletTrap`

4. In the **IP Address** field, enter the IP address of this server or click **Get address** to have FireWall-1 resolve it automatically.
5. Fill out the rest of the page, for example, **Location** (Internal, External) and **Type** (Host, Gateway) as appropriate for your circumstances.

   No particular settings are required for AppletTrap, and none of the other pages are directly relevant to this setup.
6. Click **Close** when you have finished.

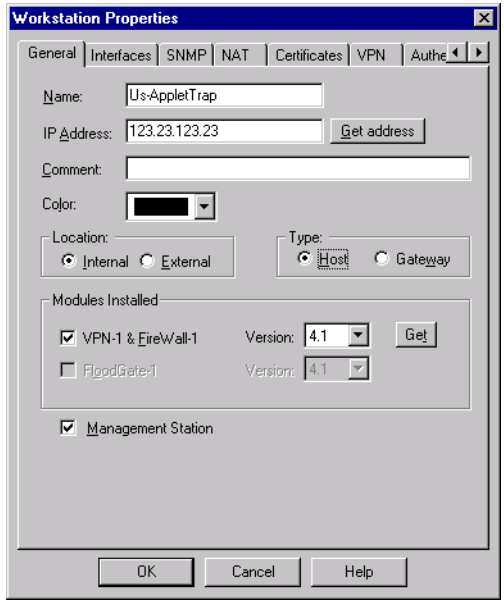


FIGURE 3-4. Create a Network Object for AppletTrap.

C. FireWall-1: Creating a Server Object

1. In the FireWall-1 configuration page, click **Manage > Servers**.
2. Click **New**, then choose **CVP** from the drop-down menu.
3. Enter a name for the Server in the **Name** field, for example, **AppletTrap_Server.**
4. Next, click the **Host** drop-down box and select the Network Object you created in task B, **`US-AppletTrap`** in our example.
5. Accept the **Service** type already specified; i.e., *FW1_cvp*.
6. Click **OK**, then **Close.**

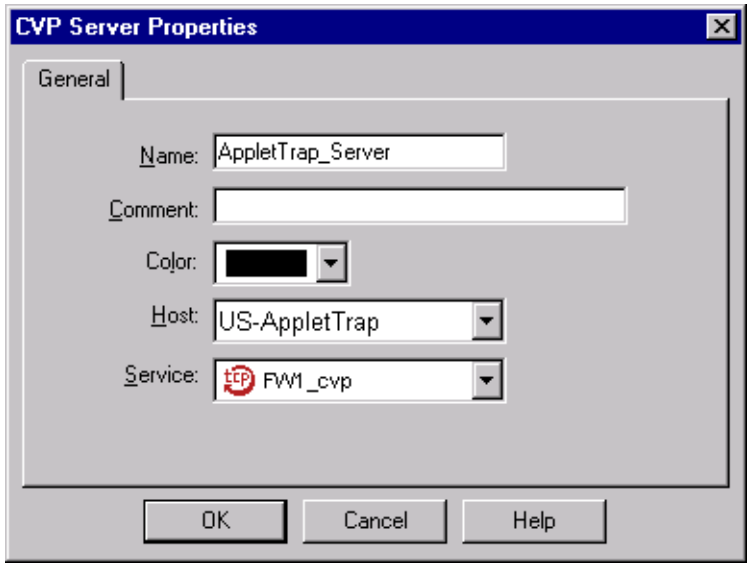


FIGURE 3-5. Define a Server Object for AppletTrap.

D. FireWall-1: Creating a Resource Object

1. In the FireWall-1 configuration page, click **Manage > Resources**.
2. Click **New**, then choose the **URI** protocol from the drop-down menu.
3. In the **General** tab, enter a name for the Resource in the **Name** field, for example, **AppletTrap_Resource**.
4. Make the **Action** tab active and, in the **Server** drop-down box, select the *Server* you created in task C, **`AppletTrap_Server`** in our example.

   Click **Read/Write**, the only valid option for AppletTrap.
5. Click **OK**, then **Close**

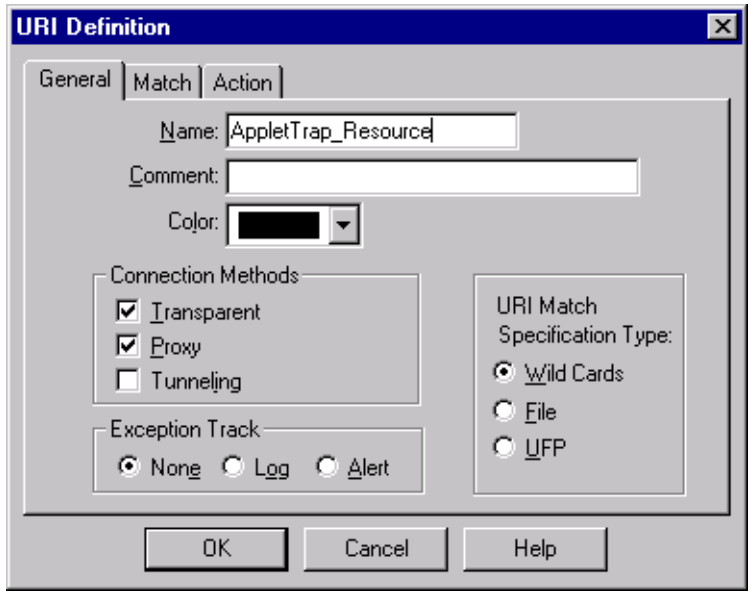


FIGURE 3-6. Define a Resource Object for AppletTrap.

E. FireWall-1: Adding a Rule to the Rule Base

1. In the FireWall-1 configuration page menu, click **Edit > Add Rule > Top** to create a new rule.
2. Next, right-click the **Service** column of the rule and choose **Add With Resource**.
3. From the list of Services, select **http** for the AppletTrap service and specify **AppletTrap_Resource**.
4. Right-click the **Action** column of the rule and choose **accept** from the menu that appears.
5. Optionally, right-click the **Track** column of the rule and then choose **Long** to enable logging.

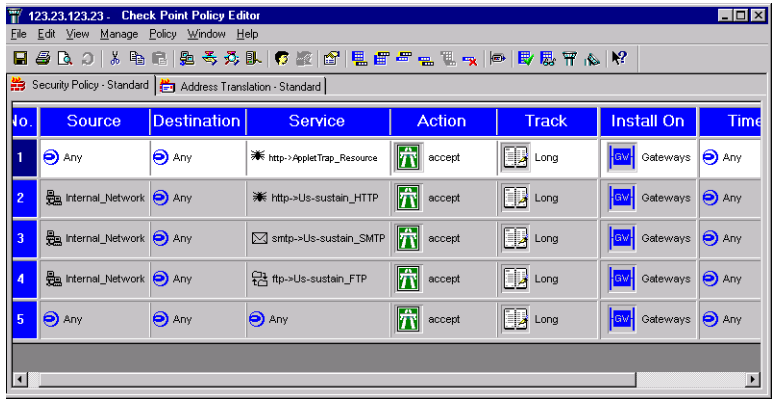


FIGURE 3-7. AppletTrap's scanning services are added to the CVP rule base.

F. FireWall-1: Installing the Rule

1. From the FireWall-1 configuration page menu, click **Policy > Install**.
2. Highlight the FireWall-1 server where you want this policy installed, and click **OK**.
3. Click **Close** to complete the operation.

Rule Base Order

FireWall-1 examines the rule base sequentially, from top to bottom, until a rule successfully matches the type of traffic being examined. We recommend that you place the AppletTrap rule accepting HTTP connections *before* any other rules which accept this service to ensure AppletTrap performs its scanning/instrumentation.

For example, if you define a rule allowing all HTTP connections, but place this rule ahead of one specifying CVP scanning on a URI Resource, *the CVP rule will never be executed*.

G. Setting up Check Point's Authentication for AppletTrap

The connection between AppletTrap and FireWall-1 can be authenticated at the transport layer using Check Point's proprietary authentication algorithm. Before

enabling the FireWall-1 authentication port in AppletTrap, you must do the following:

1. Establish an authentication key for communication between the machines. The machines identify themselves using the authentication key.
2. Establish authenticated communication between the OPSEC Client process (FireWall-1) and the OPSEC Server process (AppletTrap).

On the FireWall-1 side

1. Go to the **FireWall-1's `bin`** directory and enter the following command:

   ```
   fw putkey -opsec [IP address of the AppletTrap machine]
   ```

   You are prompted to enter a secret key. Type a sequence of at least 4 characters.

2. On FireWall-1, edit the `$FWDIR/conf/fwopsec.conf` file to show that the connection from AppletTrap is authenticated. The server IP address or hostname should point to the AppletTrap machine corresponding to the OPSEC port and "auth_opsec" should be set. For example,

   ```
   server 123.22.33.44 18181 auth_opsec
   ```

   should be changed to:

   ```
   server AppletTrap 18181 auth_opsec
   ```

On the AppletTrap side

Run the `opsec_putkey` program and then open the AppletTrap configuration page to enable **Authenticated OPSEC Connections**:

1. The `opsec_putkey.exe` program needs to be run with the following command line options:

   ```
   opsec_putkey [IP address of FireWall-1]
   ```

   You will be prompted to enter the secret key, which was configured on the FireWall-1 side.

2. Once `opsec_putkey` is successful, some **`*.c`** files will be created (`for example, authkeys.C` or `rand.C`). These files must be copied into the same directory as the `AppletTrap` program files.

Chapter 4

Getting Started

This chapter contains information on how to get started with AppletTrap. Topics include:

- Defining the thread pool (Standard version)
- Setting Network and HTTP timeout values (Standard version)
- Enabling authenticated OPSEC connections (FireWall-1 version)
- Enabling large file trickle (FireWall-1 version)
- Changing the system password
- Choosing security options for handling mobile code
- Stopping/restarting the InterScan AppletTrap proxy server

Server Administration

Setting the Maximum Number of Server Threads (Standard version)

This option defines the InterScan AppletTrap thread pool. The thread pool is static and services all HTTP client requests. The number you set for this parameter will limit the total number of concurrent requests that InterScan AppletTrap will accept; requests in excess of this number are queued. The larger the number you assign, the more memory will be devoted to threads.

Each element (i.e., each GIF, applet, etc.) of a Web page uses its own thread. Therefore, in defining InterScan AppletTrap's thread pool, choose a number that represents an equitable balance between available system resources and performance; i.e., one that can reduce the need for queuing. By default, the system thread pool is set to 30.

To set the server threads...

1. From the left pane, select **Server Administration**. The Server Administration page appears on the right pane:
2. Enter the value you prefer in the **Max number of server threads** text box.
3. Scroll down and click **Apply**.

Setting Network and HTTP Timeout Values (Standard Version)

There are two user-adjustable timeouts, one for network connection and the other for HTTP connection. The defaults are 300 seconds for **Network read timeout** and 120 seconds for **HTTP keep-alive timeout**. To modify the timeout values, just type in a new value and click **Apply**. Values are measured in seconds.

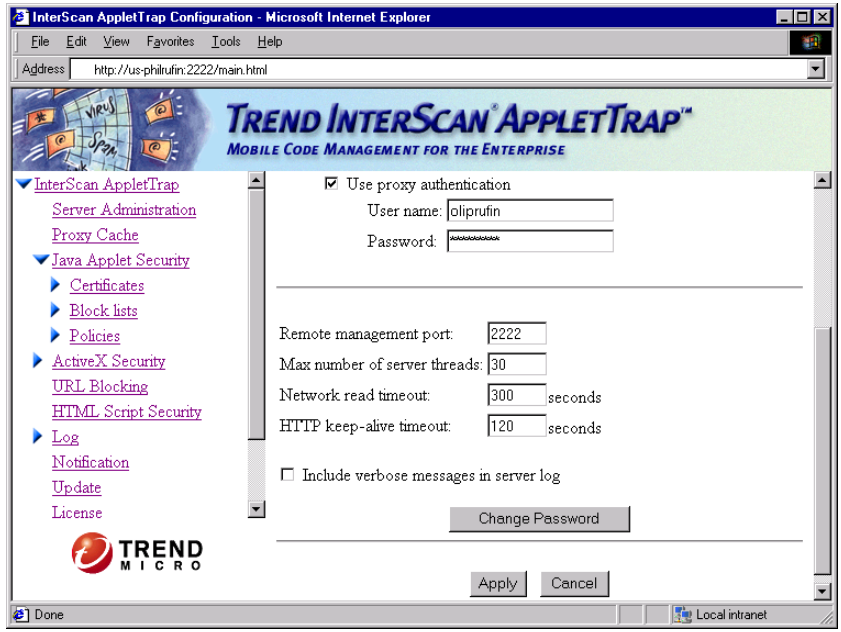


FIGURE 4-1. The configuration page for specifying the InterScan AppletTrap proxy server configuration (Standard version).

Enabling Authenticated OPSEC Connections (FireWall-1 Version)

To change the default settings...

1. From the left pane, select **Server Administration**. The Server Administration page appears on the right pane.
2. Select the **Enable authenticated OPSEC connections** checkbox if your FireWall-1 server is configured for authentication. OPSEC stands for the Open Platform for Security. Open Platform for Security is a single platform architecture designed to allow integration and management of all aspects of network security through an open extensible framework.

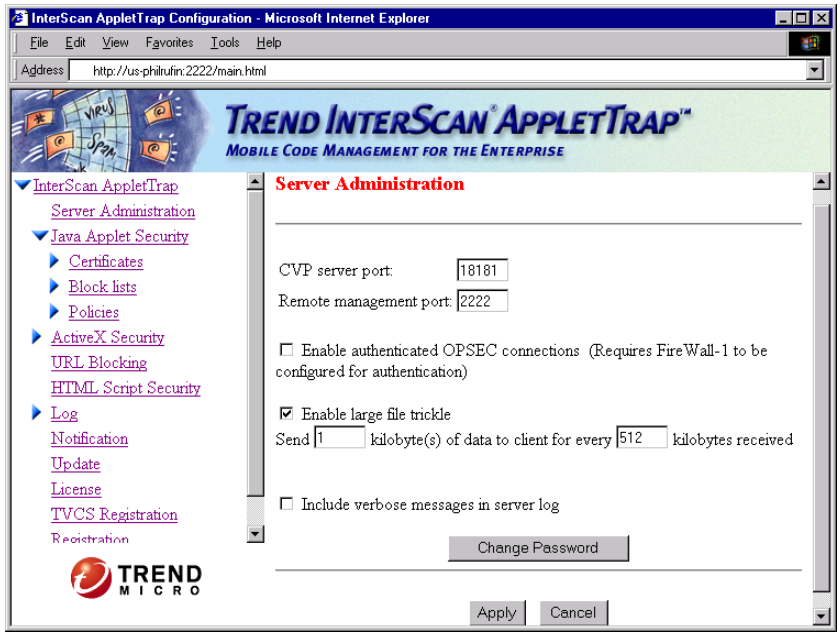


FIGURE 4-2. The Server Administration configuration screen (FireWall-1 version).

Enabling Large File Trickle (FireWall-1 version)

Select the **Enable large file trickle** checkbox if you are experiencing "timeout" issues when downloading large files. "Trickle" sends small amounts of data to the requesting client in advance of transferring the entire scanned file. Specify the number of kilobytes of data to send for a specified number of kilobytes received.

Setting Up Security

InterScan AppletTrap implements password protection to prevent unauthorized access and modification of the system configuration.

By default, each InterScan AppletTrap proxy server is protected by the password **trend**. This value is case-sensitive. We recommend that you change this password immediately after installation as other users may already have read it in the manual.

To modify the password...

1. Click **Change Password**. The Change Password screen appears.
2. Taking note that the password is case-sensitive, enter a new password in the **Type password** text box, confirm your choice in **Re-type password**, then click **OK**.
3. Click **OK** on the next screen.

InterScan AppletTrap will prompt you to log on again to continue with the system administration. When prompted, specify the same user name (i.e., **admin**) and the new password you just set.

Choosing Security Options for Handling Mobile Code

InterScan AppletTrap provides various security options for handling Java applets, HTML scripts, and ActiveX controls. The following describes the configurable options available for each type of mobile code.

Configuring Java Applet Security

InterScan AppletTrap blocks known malicious applets based on the following lists:

- A **downloadable hash list** from Trend Micro containing the identification of known malicious applets. This list is included by default on the system, and is automatically updated during Internet updates.
- A **user-configurable hash list** containing the identification of malicious applets manually added to the list. InterScan AppletTrap also automatically updates this list to include any malicious applets detected on client workstations.
- A **user-configurable URL list** containing specific URLs that are known sources of malicious applets and HTML scripts.

As Java applets are downloaded to the proxy server, InterScan AppletTrap compares them with the above block lists. Any applets found in the lists are immediately discarded and, in their place, InterScan AppletTrap creates a new applet that displays the following message when delivered to client workstations: **This applet is identified to violate security policy and is blocked**.

In the case of attempts to access a restricted site, the system creates a new HTML page containing the message: **The URL <URL address> is blocked by InterScan AppletTrap**. This new page is delivered to client workstations in place of the original page.

For Java applets, you can configure the following options:

- Enable or disable use of the user-configurable hash list and user-configurable URL list in the filtering process. The downloadable hash list is always enabled.
- Enable or disable immediate blocking of all malicious applets the system automatically adds to the user-configurable hash list.
- Enable or disable applet instrumentation. Disabling this feature turns off real-time applet scanning protection on client workstations.
- Select whether or not to re-sign instrumented applets. If you have this feature enabled, make sure that you have the proper signing key imported to the system and to the Web browsers of your clients. For information on how to do this, please see the **Importing a Signing Key** section.

Note: Re-signing only applies to signed applets. If the system is configured to accept unsigned applets, these applets will bypass this process and will be delivered to client workstations immediately after instrumentation.

- Block or accept unsigned applets. Blocking unsigned applets enables certificate checking for all Java applets downloaded at the server.

By default, InterScan AppletTrap uses all the block lists in the filtering process, blocks all recently added applets to the user-configurable hash list, instruments and re-signs applets, and accepts signed and unsigned applets.

Modifying the security options for Java applets

1. From the left pane, select **Java Applet Security**. The Java Applet Security page appears on the right pane.
2. To enable the security options provided on this page, select the **Enable the following Java Applet security protection** checkbox.
3. Under **Block List**, select the provided checkbox to enable the immediate blocking of those applets the system automatically adds to the user-configurable hash list.
4. To monitor the behavior of applets in real time, select the **Instrument applets** checkbox under **Applet Instrumentation**.
5. Under **Digital Signing**, do the following:

- To re-sign instrumented applets, select the **Re-sign applets** checkbox. You do not need to enable this feature if you have the applet instrumentation function disabled in the **Instrument applets** checkbox.
- Select the **Disallow unsigned applets** checkbox to prevent applets with unrecognized certificates from entering the proxy server. Clearing this checkbox basically disables certificate verification for this mobile code.

6. Scroll down and click **Apply** to save the new configuration or **Cancel** to ignore the changes and use the previous settings.

To view the Trend hash list...

1. From the left pane, expand **Java Applet Security** and then **Block lists**.
2. Select **Trend Hash List**. The Trend Hash list is always enabled.

To enable the user-configurable hash list...

1. From the left pane, expand **Java Applet Security** and then **Block lists**.
2. Select **User Hash List**. The configuration page for this option appears on the right pane.
3. Check the **Enable this block list** checkbox at the top of the screen.
4. The check mark at the left of each entry signifies that the applet is currently blocked. You can disable an entry by clearing the checkbox and clicking **Apply**.
5. Click **Apply** to save your changes

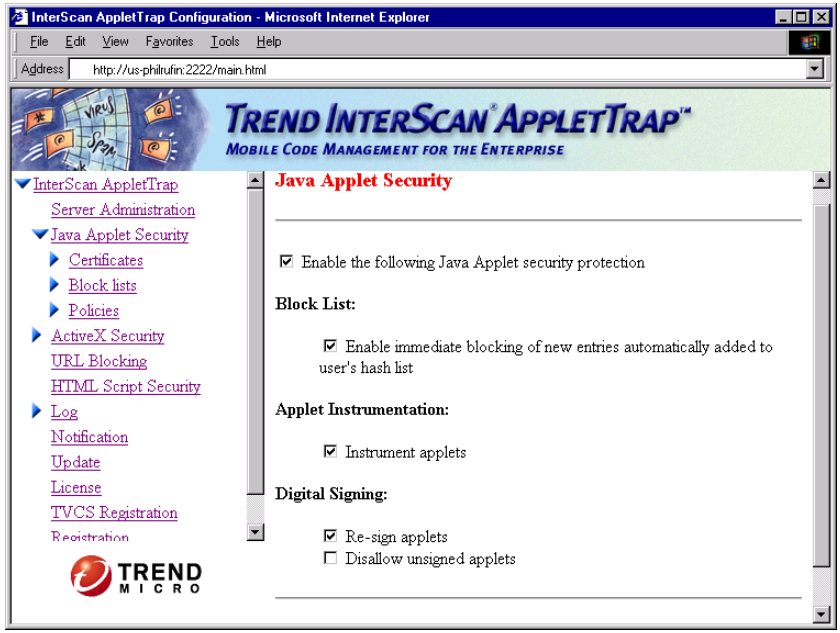


FIGURE 4-3. The configuration page for setting the Java applet security options.

Configuring ActiveX Security

For ActiveX controls, you can configure the following options:

- Select the ActiveX files to be blocked at the server. You have the option to block either or both of the following file formats commonly used by ActiveX controls: Portable Executable (PE) and Cabinet (CAB).

> **Note:** Remember that all accepted ActiveX controls still need to pass through the certificate verification process before they are sent to client workstations.

- Save all ActiveX controls into a specific directory for later importation into the certificate database of Microsoft Internet Explorer. InterScan AppletTrap uses this database to filter unsecured ActiveX controls.

Note: The ActiveX authenticode feature only exists on Microsoft Windows environment; and is not available on Solaris version. You need the Windows registry to get the ActiveX authenticode information.

By default, InterScan AppletTrap blocks all Cabinet-formatted files and saves those with unrecognized certificates in the **c:\temp** directory at the server.

To configure ActiveX security...

1. From the left pane, select **ActiveX Security**, then **Authenticode Validation**. The ActiveX Security page appears on the right pane:

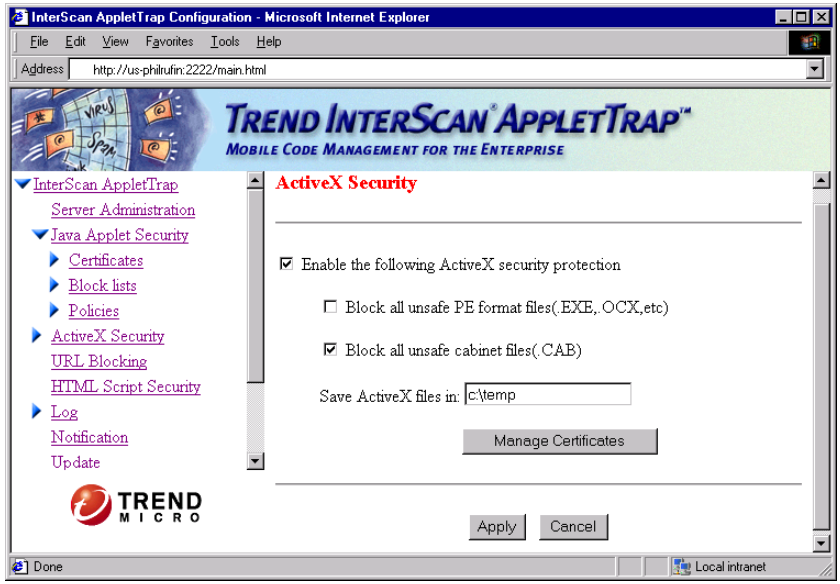


FIGURE 4-4. The configuration page for setting the ActiveX security options.

2. Select the **Enable the following ActiveX security protection** checkbox to enable the security options provided on this screen.
3. Select the checkbox(es) for the ActiveX files you want to block:

- Select **Block all unsafe PE format files** to block all PE-formatted files; e.g., EXE and OCX.
- Select **Block all unsafe cabinet files** to block all Cabinet-formatted files. Cabinet files come with the CAB extension.

Note: The settings you specify here do not just apply to ActiveX controls — they will also be applied to other files of the same file type. For example, selecting both checkboxes will block all files with extensions EXE, OCX, CAB, etc.

4. Specify a directory in the **Save ActiveX files in** text box for saving ActiveX controls that are blocked.
5. Click **Apply**.

For information on how to import the saved certificates into Internet Explorer, please see the section "Modifying the Internet Explorer's Certificate Database from the Administrator Console" in Chapter 6, "Configuring InterScan AppletTrap".

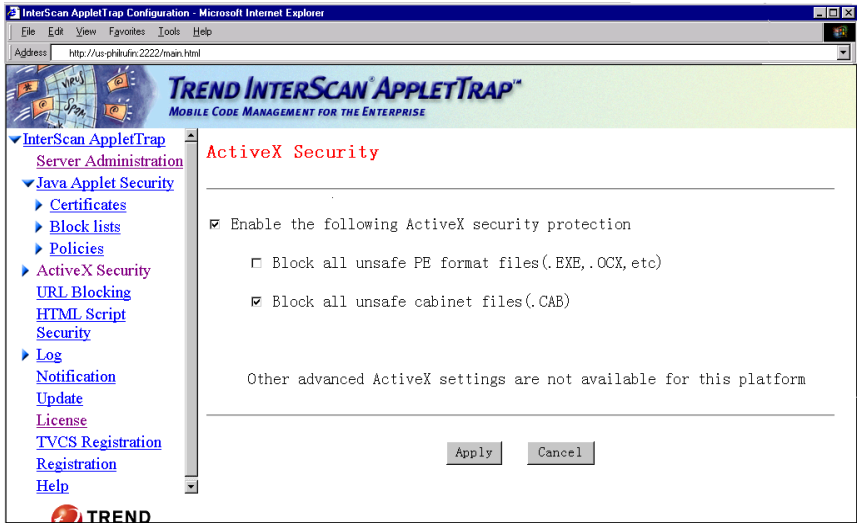


FIGURE 4-5. The configuration page for setting the ActiveX security options (Solaris version).

To view the Trend hash list...

1. From the left pane, expand **ActiveX Security** and then **Block lists**.
2. Select **Trend's List**.

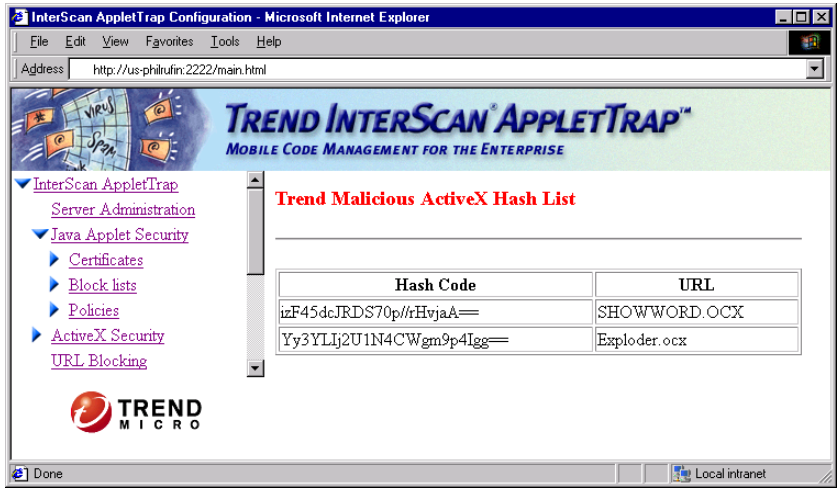


FIGURE 4-6. Viewing Trend Micro Malicious ActiveX Hash list.

To enable the user-configurable hash list...

1. From the left pane, expand **ActiveX Security** and then **Block lists**.
2. Select **User Hash List**. The configuration page for this option appears on the right pane.
3. Check the **Enable this block list** checkbox at the top of the screen.
4. The check mark at the left of each entry signifies that the applet is currently blocked. You can disable an entry by clearing the checkbox and clicking **Apply**.
5. Click **Apply** to save your changes.

Configuring URL Blocking

This feature works correctly only if FireWall-1 is configured to work with an HTTP proxy. If there is no HTTP proxy, it is recommended to disable the URL Blocking.

To configure URL Blocking,

1. Select **URL Blocking**.
2. The check mark at the left of each entry signifies that access to that site is currently restricted. You can disable an entry by clearing the checkbox.
3. Check **Enable this block list** to use this list in the URL filtering process.

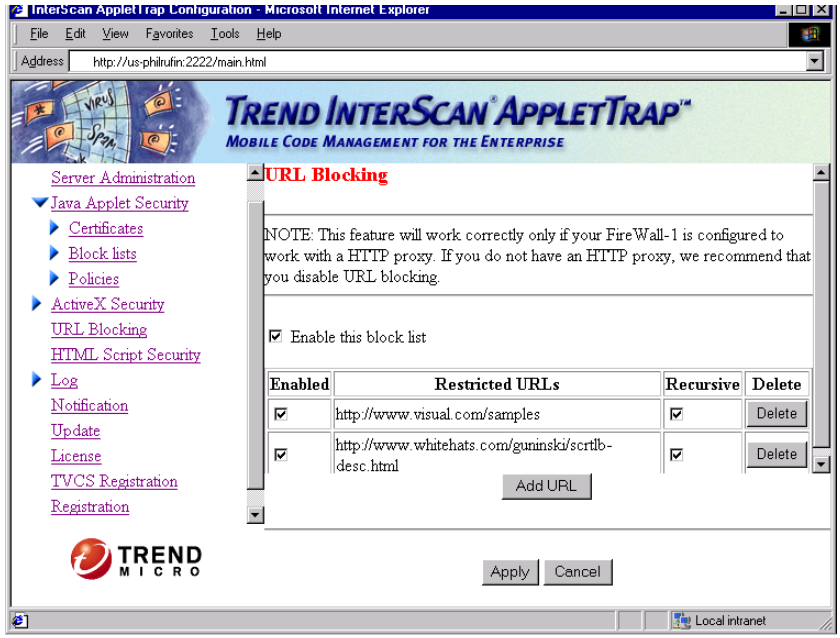


FIGURE 4-7. URL Blocking Configuration Screen (FireWall-1 version).

4. Click **Add URL**.
5. On the next prompt, enter the URL that you want to be restricted from client access, then click **OK**.

Note: Do not forget to include **http://** before the address.

6. Select the **Recursive** checkbox if you would like to block all URLs that are included under this URL.
7. Repeat the same procedure to add other URLs.
8. Click **Apply** to save the new list.

Configuring HTML Script Security

You have the options of filtering all HTML languages or allowing all HTML languages to pass. When the feature of filtering all HTML script languages is enabled, InterScan AppletTrap restricts access to specific Web sites that are known sources of malicious code. As script filtering takes up a certain amount of time and system resources, the feature of allowing all HTML languages to pass is enabled by default.

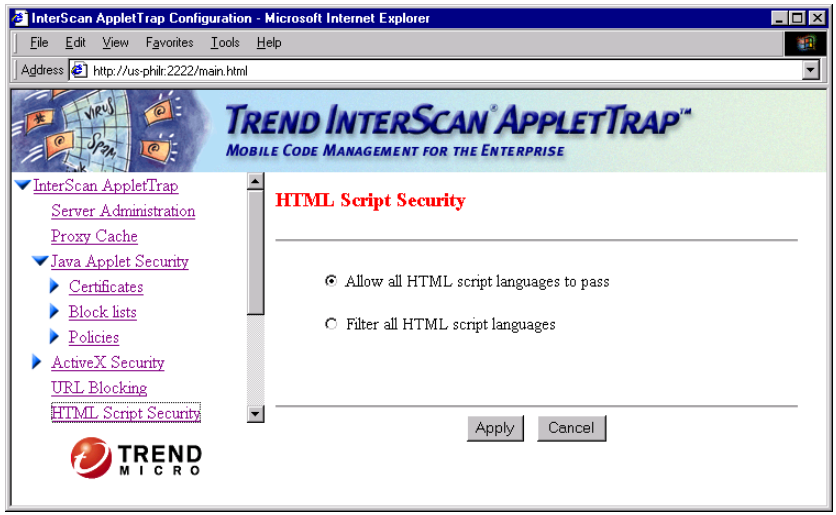


FIGURE 4-8. The configuration page for setting the HTML Script security option.

To configure HTML Script security...

1. From the left pane, select **HTML Script Security**.
2. To allow all HTML script languages to pass, select the **Allow all HTML script languages to pass** checkbox.
3. Alternatively, select **Filter all HTML script languages** if you would like to filter out JavaScript, VBScript, and all other script languages.
4. Click **Apply**.

Stopping/Restarting the InterScan AppletTrap Proxy Server

You can temporarily stop the InterScan AppletTrap proxy server to disconnect your clients from the Internet while you are modifying your network topology, or while you are specifying a new configuration for the InterScan AppletTrap proxy server. By doing this, you can make sure that no malicious mobile code goes through unchecked while the configuration is being modified.

To stop/start InterScan AppletTrap (Standard version):

1. From the left pane, select **InterScan AppletTrap**. The configuration page for this option appears on the right pane.
2. Click **Stop** or **Start AppletTrap**.

The screen displays the new server status. InterScan AppletTrap resets the statistics counters for the current session when AppletTrap is restarted.

To stop/start InterScan AppletTrap (FireWall-1 version):

1. Go to Windows **Start > Settings > Control Panel > Services**.
2. From the list of services, click on **InterScan AppletTrap**.
3. Click the **Start** or **Stop** button.

InterScan AppletTrap resets the statistics counters for the current session when you restart the service.

To stop/start InterScan AppletTrap (Solaris version):

1. Change the directory:

```
cd /opt/trend/InterScan_AppletTrap/
```

2. To stop the service:

```
#/opt/trend/InterScan_AppletTrap/
apptrap.init stop
```

3. To restart the service:

```
#/opt/trend/InterScan_AppletTrap/
apptrap.init start
```

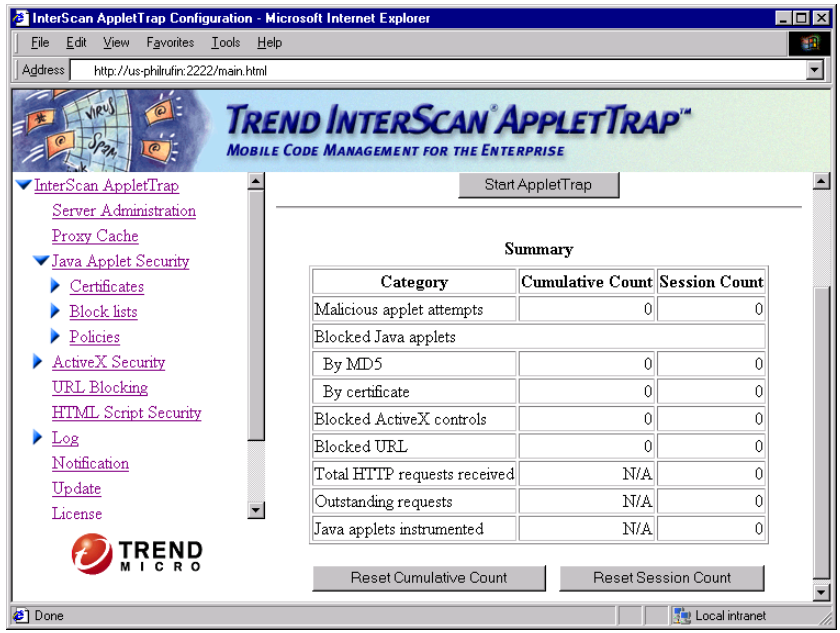


FIGURE 4-9. To stop/start InterScan AppletTrap (Standard version).

Chapter 5

Creating & Mapping Security Policies

Security policies, which work in conjunction with monitoring codes, control the behavior of applets on client workstations. Based on a policy, InterScan AppletTrap may or may not allow the operation to execute. InterScan AppletTrap allows you to customize policies that will best fit your client needs. In this chapter you will learn how to create and map policies, which best serve the set of users. This chapter contains detailed information on:

- System Security Policies
- Creating Security Policies
- Mapping Security Policies

System Security Policies

InterScan AppletTrap uses a set of rules, called **security policies**, to control the behavior of applets on client workstations. These security policies work in conjunction with monitoring codes, which extract information about the resources applets will use. Both are inserted into the applet's code during the instrumentation process.

Upon delivery to a client workstation, the monitoring codes extract the resource information and then determine whether the operation is permitted by comparing it with the attached security policy. Based on this policy, InterScan AppletTrap may or may not allow the operation to execute.

Since a single policy is not appropriate for all applets or users, InterScan AppletTrap allows you to customize policies that will best fit your client needs. For example, while unknown applets should not generally be given access to the corporate directory server, some of your clients may require applets from business partners to have access to this resource. You can create and map a policy that will best serve this set of users, and map a different policy to other clients.

By default, InterScan AppletTrap maps a factory-set security policy for all its clients. This default policy has the following rules:

File Access

- Non-destructive file operations such as listing files in a directory and retrieving file attributes are disabled for all files
- Destructive file operations such as deleting and renaming files are disabled for all files
- Reading file contents is disabled for all files
- Writing to files is disabled for all files

Network Access

- Allow applets to connect to their originating hosts
- Prevent applets from connecting to any other hosts

Threads

- Allow a maximum of eight threads for each applet

Windows

- Limit each applet to a maximum of five active windows

The default security policy should work in most network environments and should be used until your business or clients' requirements change. However, if your prefer, you can create new ones for different groups of users in your network.

There is no limit to the number of policies you can create. Remember though that each policy eats up memory space on your hard disk, although it is very minimal. After creating a policy, map it to the client or group of clients you want to use this policy. InterScan AppletTrap only uses those policies that are mapped to clients.

To help illustrate the policy creation process, let's use the sample topology given in the figure below.

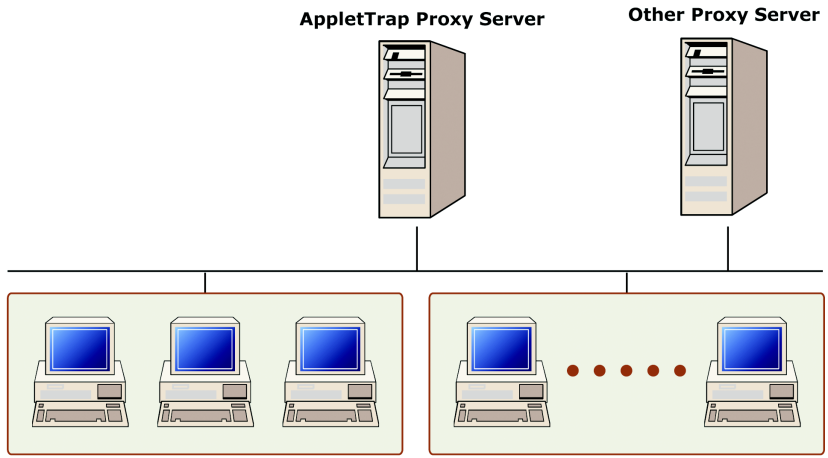


FIGURE 5-1. Sample network topology for creating security policies.

Creating Security Policies

Based on the sample topology in Figure 5-1 above, we only need to create one security policy (i.e., for the RND group). The other group will use the factory-set policy, **medium**.

To create a policy...

1. From the left pane, expand **Java Applet Security** and then **Policies**.
2. Select **Define Policies**. The Define Policies page appears on the right pane:

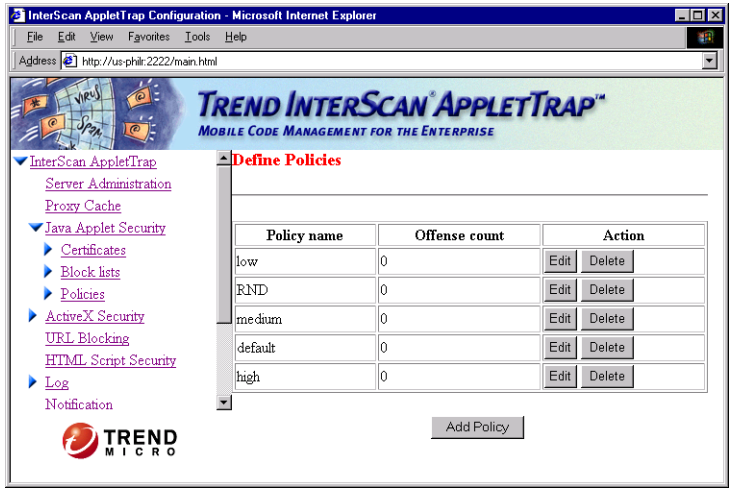


FIGURE 5-2. The configuration page for creating, modifying, and deleting security policies.

In addition to the **default** policy, InterScan AppletTrap also comes with three other factory-set policies for low, medium, and high security settings. These extra policies, however, are not mapped. To display the settings for a particular policy, click its corresponding **Edit** button.

The **Offense count** column on the table above displays the number of malicious offenses detected for each policy.

3. Click **Add Policy** and assign a name for the policy you want to create on the next screen. For this example, enter **RND** and then click **OK**.

FIGURE 5-3. The screen to specify the rules for a particular security policy.

4. Select the **File I/O** tab. This tab allows you to set the rules for file operations.

   Enter the following values:

   - The **Non-destructive file system operations** group applies to those operations that do not modify the file systems in any way (e.g., listing files in a directory and getting file attributes).

     To enable these operations for all files, select the **Enabled for all files** option button. To disable, select the **Disabled for all files** option. You can also specify exceptions by using the corresponding **Exception** button.

     For our example, select **Enabled for all files** then click **Exception**. Click **Add** on the next screen, and then enter **C:\DATABASE**, select **Include all subfolders and files**, and click **OK** on the next to add the entry into the

Exception list. To modify a particular entry in this list, select the option button, then click **OK**.

- The **Destructive file system operations** group applies to those operations that make permanent changes to the file systems such as deleting and creating files and directories.

  For our example, let's disable these operations for all files by selecting the **Disabled for all files** option.

- The **Reading file contents** group applies to operations that read the file contents.

  Select **Enabled for all files** for our example.

- The **Writing to files** group applies to those operations that modify the file contents.

  Enable this feature for our example by selecting **Enabled for all files**.

5. Select the **Network** tab. This tab allows you to set the rules for network operations.

   Enter the following settings:

   - To allow applets to bind the local ports, select the **Allow applets to bind local ports** checkbox. This enables applets to manipulate the services that are bound to the clients' service ports. To disallow this operation, leave this checkbox blank.

     For our example, let's allow binding to local ports.

   - To allow applets to connect to their originating hosts, select the **Allow applets to connect to their originating servers** checkbox. Otherwise, clear this checkbox.

     For our example, let's use the default setting of allowing applets to connect to their originating hosts.

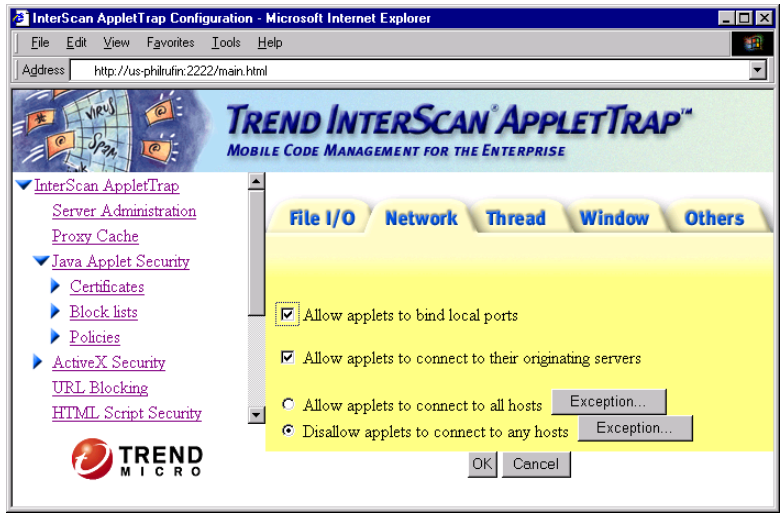


FIGURE 5-4. The tab for setting rules for network operations.

- The next two options determine whether or not to allow applets to connect to hosts other than the ones they originated from.

  To permit this operation, select the **Allow applets to connect to all hosts** option button. To disallow it, select the **Disallow applets to connect to any hosts** option. You can also specify exceptions using the corresponding **Exception** button.

  For our example, let's use the default setting of not permitting applets to connect to any other hosts.

6. Select the **Thread** tab to set the rules for creating new thread groups and limit the number of threads applets can create.

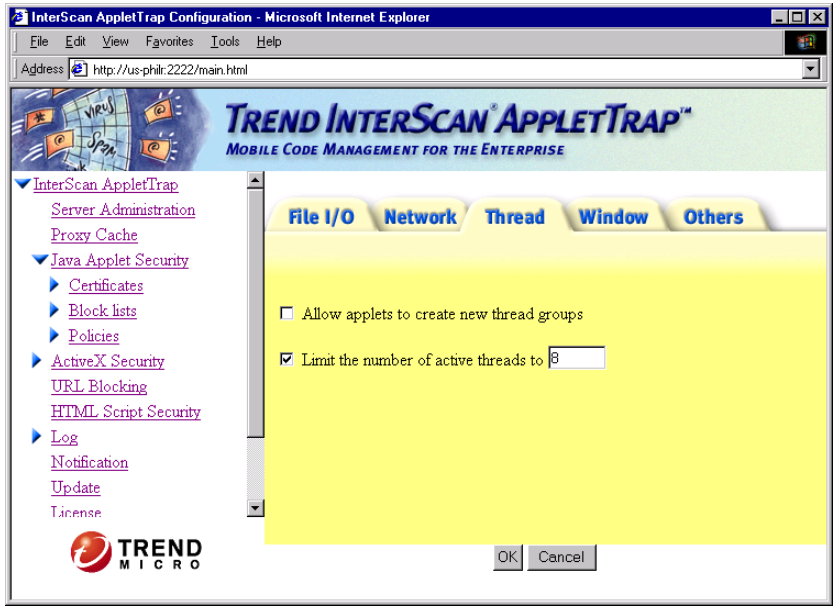


FIGURE 5-5. The tab for specifying whether or not to allow applets to create new thread groups and number of active threads they can create.

Enter the following settings:

- Select the **Allow applets to create new thread groups** checkbox if you want to allow applets to perform such an operation. This gives applets permission to manipulate threads outside their own thread groups. To disallow this operation, clear this checkbox.
- To restrict the number of active threads applets can create, select the **Limit number of active threads to** checkbox and then specify in the provided text box the allowable number of threads. Clearing this option gives applets the freedom to open as many threads as they want.

  For our example, let's use the default settings to prevent applets from creating new thread groups and limit the active threads to eight.

7. Select the **Window** tab. This tab allows you to specify the maximum number of windows applets can open.

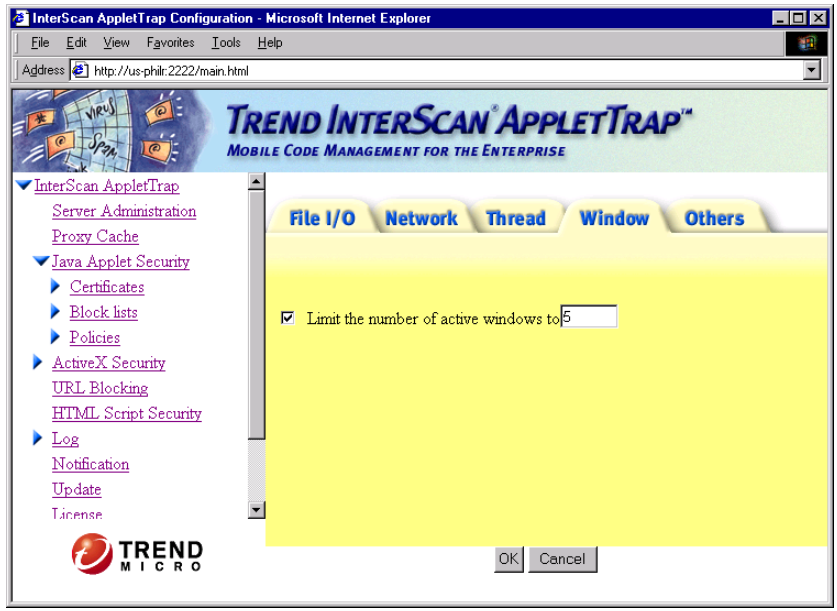


FIGURE 5-6. The tab for specifying the maximum number of active top-level windows applets can open.

Enter the following setting:

- Select the **Limit number of active windows to** checkbox if you want to limit the number of active top-level windows applets can open. Enter the number of allowable windows in the provided text box. Clearing this option gives applets the freedom to open as many windows as they want — just like some malicious Java applets do to annoy users.

  For our example, let's use the default setting of allowing applets to open a maximum of five windows.

8. Select the **Others** tab. This tab determines how InterScan AppletTrap should interact with clients upon detection of malicious applets and how to handle non-standard Java packages, such as **NETSCAPE.*** and **COM.MS**.

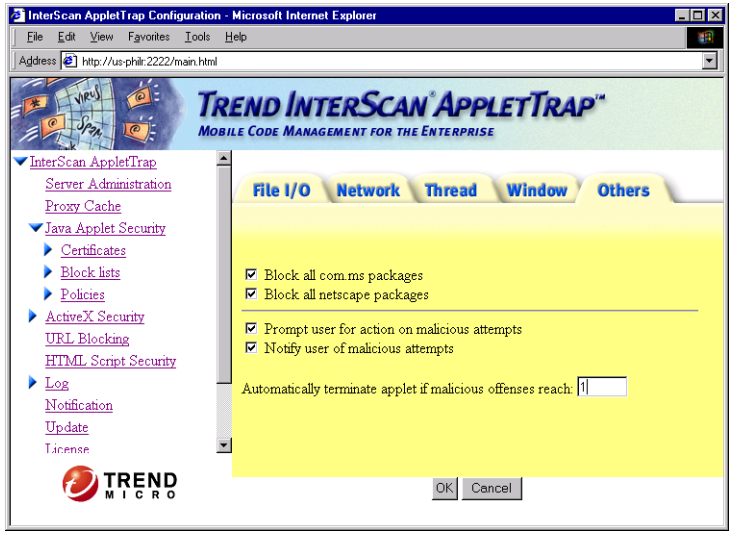


FIGURE 5-7. The tab for enabling or disabling client action and protection against non-standard Java packages.

Enter the following settings:

- To enable protection against non-standard Java packages, check the **Block all com.ms packages** and **Block all netscape packages** checkboxes. **COM.MS** runs on Internet Explorer, whereas **NETSCAPE.*** runs on Netscape Web browsers. These packages are potential threats because they can access the Windows native operating system resources.

  For our example, let's enable these features.

  Note: For security reasons, the system does not block the **NETSCAPE.SECURITY** package.

- Select the **Prompt user for action on malicious attempts** checkbox if you want your clients to decide whether or not to allow malicious acts to continue. If your clients have knowledge of malicious Java applets and know how to

deal with them, enable this feature. Otherwise, clear this checkbox to leave the decision making to InterScan AppletTrap. When enabled, InterScan AppletTrap displays a message similar to the following when it detects malicious behavior on the client workstation:

Figure 5-8. Applet alert that AppletTrap displays when it detects malicious behavior on client workstations, and client action is enabled.

From this screen, the client has the option to allow or disallow the action (i.e., current thread) from continuing, or terminate the entire applet. An applet may create more than one thread.

When disabled, InterScan AppletTrap instead displays a screen similar to the following:

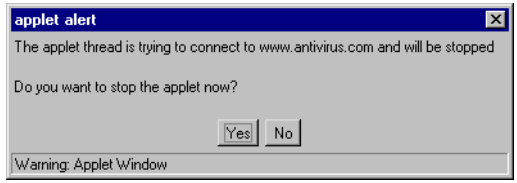


Figure 5-9. Applet alert that InterScan AppletTrap displays when client action is disabled.

From this screen, the client has the option to either terminate the current thread or the entire applet.

For our example, let's leave the decision making to clients by selecting **Prompt user for action on malicious attempts**.

- To notify clients of malicious applet behavior, select the **Notify user of malicious attempts** checkbox. You need to enable this feature to have the above screens appear on client workstations. Otherwise, InterScan AppletTrap would just terminate any malicious act upon detection.

For our example, we use the default settings to notify the clients.

- To automatically terminate applets based on the malicious offenses they commit, enter a value in the provided text box.

  Since an applet may create more than one thread and clients, if given authority, may allow malicious actions to continue, you need to limit the number of malicious offenses applets can do.

  This option only becomes relevant when the **Prompt user for action on malicious attempts** checkbox is selected.

9. Click **OK** to save the new policy.

Mapping Security Policies

After creating the policies you need, map them to their respective clients. The following describes the policy mapping procedure for the sample network topology given in Figure 5-1 with some example options filled in.

To map security policies...

1. From the left pane, expand **Java Applet Security** and click **Policies**. Then select **Map Policies**. The Map Policies page appears on the right pane.

   By default, this screen only contains one entry. The asterisk "*" under the **Domain** or **IP** field means that the policy **default** is mapped to all clients of this InterScan AppletTrap proxy server.

   The order in which entries appear on this screen is significant — when deciding which policy to attach for a particular client, InterScan AppletTrap starts with the first entry on the list, checking whether it matches the client's domain name or IP address. If a match is not found, InterScan AppletTrap goes on to the next entry and so on until a match is found.

   To ensure that all your clients have a policy set for them, InterScan AppletTrap always keeps the default entry at the end of the list (i.e., all entries you add will be placed before the default entry). Therefore, if you forget to assign a policy to a client, InterScan AppletTrap will automatically use the default policy.

   For our example, let's arrange the entries in the following order: 1) RND mapping and 2) **medium** policy for the specified IP addresses.

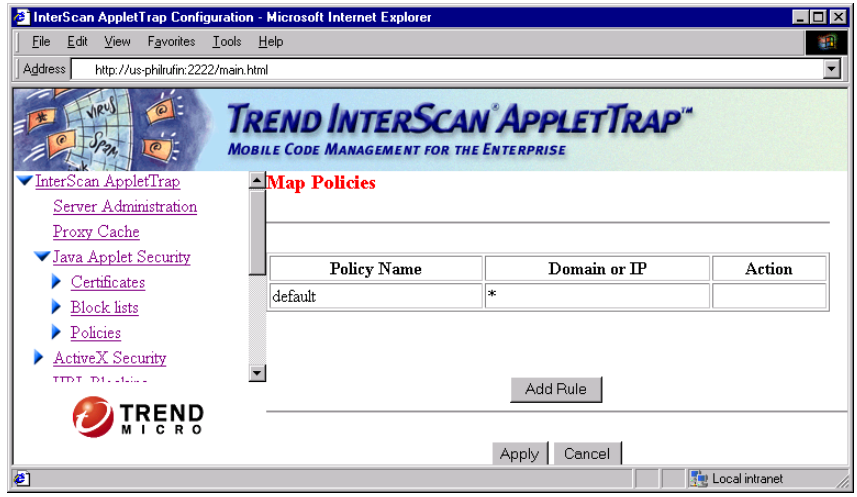


FIGURE 5-10. The configuration page for mapping policies.

2. Click **Add Rule**. The following screen appears:

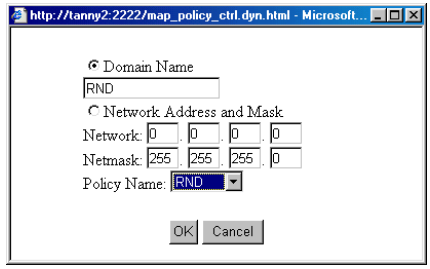


FIGURE 5-11. The screen for mapping security policies.

3. Select **Domain Name** and then enter **RND** in the provided text box.

Note: The system supports the asterisk "*" wildcard character for mapping a particular policy to all InterScan AppletTrap clients.

In the **Policy Name** drop-down list box, select **RND** and then click **OK** to add the new mapping to the list.

4. Click **Add Rule** again and then select **Network Address and Mask** this time.

   Enter **123.45.123.0** in the **Network** text boxes, and **255.255.255.240** in the **Netmask** field. The subnet mask determines the IP address range. For information on how to compute the subnet mask, please refer to your TCP/IP documentation.

   Select **medium** from the **Policy Name** drop-down list box.

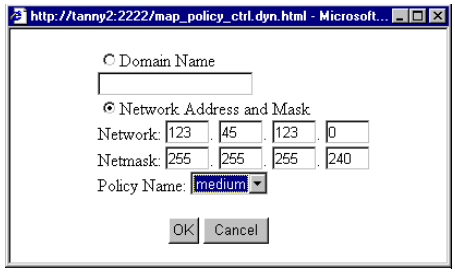


FIGURE 5-12. Mapping a policy to a group of clients using IP addresses and subnet mask.

   Click **OK** to add the new mapping to the list.

5. Use the **MoveUp** or **MoveDown** button to position the new entry between **RND** and **default**.

6. If you want to modify a particular entry, use its corresponding **Edit** or **Delete** button.

7. Click **Apply** to save the new configuration.

Sample Scenario: How InterScan AppletTrap Uses Policy Mapping

Using the list in Figure 5-13 above, let's assume that InterScan AppletTrap is instrumenting an applet that will be sent to a client whose IP address is 123.45.123.67 and who belongs to the SALES domain. The following events will occur:

1. InterScan AppletTrap checks the policy mapping to decide which policy to attach to the instrumented applet.
2. InterScan AppletTrap checks the first entry on the list (i.e., the **RND** entry). Since this entry only applies to clients in the RND domain, InterScan AppletTrap goes to the next entry on the list.
3. The second entry only applies to users with IP addresses 123.45.123.0 to 123.45.123.15. InterScan AppletTrap goes to the last entry.
4. Since this entry applies to all users, InterScan AppletTrap attaches the specified policy (i.e., **default**) to the instrumented applet

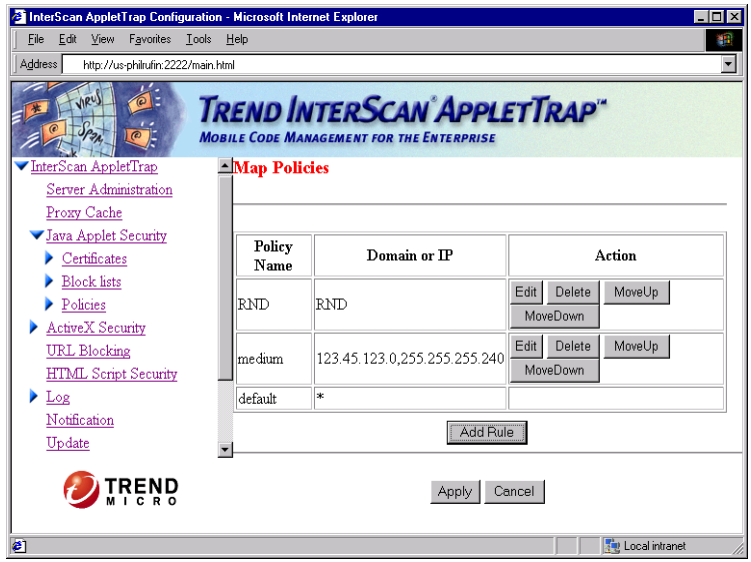


FIGURE 5-13. A sample mapping list.

Chapter 6

Configuring InterScan AppletTrap

This chapter contains information on:

- Configuring the Hash Block Lists
- Updating the user-configurable block lists
- Maintaining the InterScan AppletTrap & Internet Explorer Certificate databases
- Importing a Java Applet Signing Key
- Maintaining and ActiveX Certificate database
- Configuring notification messages

Configuring the Hash Block Lists

InterScan AppletTrap uses four updateable hash block lists to filter known malicious Java applets and ActiveX controls at the server:

- Java applet downloadable hash list
- Java applet user-configurable hash list
- ActiveX downloadable hash list
- ActiveX user-configurable hash list

Chapter 4, "Getting Started" describes the procedure on how to enable the blocking of applets and ActiveX controls using these four lists. This chapter goes into further detail on how to update the user-configurable hash lists and how to update the Java applet and ActiveX certificate databases.

Updating the User-Configurable Block Lists

The downloadable hash list is automatically updated during Internet updates. You can manually add known malicious applets and their URLs to the user-configurable block lists.

To update the user-configurable Java Applet and ActiveX hash lists...

1. From the left pane, expand **Java Applet Security** and click **Block lists** or click **ActiveX Security** and then **Block List**.
2. Select **User Hash List**. The configuration page appears on the right pane. The check mark at the left of each entry signifies that the applet is currently blocked. You can disable an entry by simply removing the check from its corresponding checkbox.

Note: Entries automatically added to this list are enabled by default. You can, however, configure the system to disable these entries by clearing the **Enable immediate blocking of new entries automatically added to user's hash list** option on the Java Applet Security configuration page.

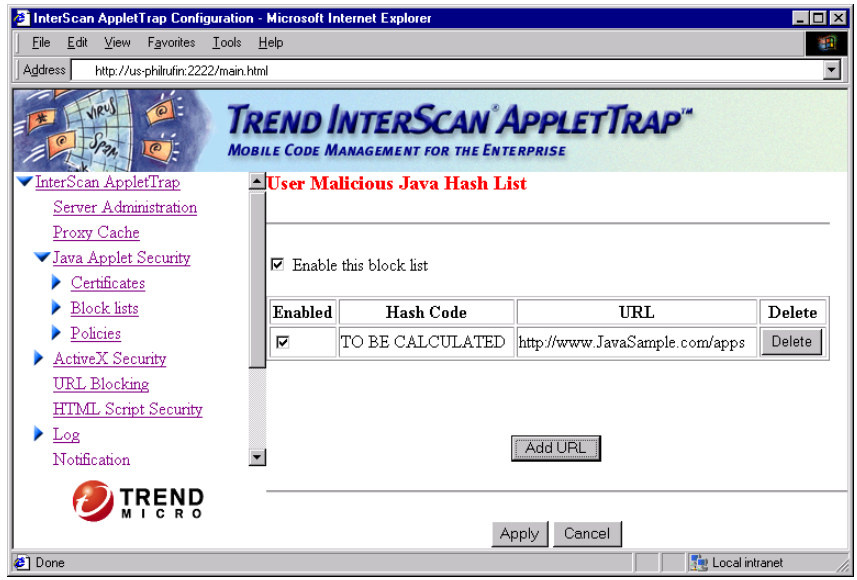


FIGURE 6-1. The configuration page for manually adding the hash codes of known malicious applets.

3. To use this list in the filtering process, select the **Enable this block list** checkbox.
4. Click **Add URL**. On the next screen, enter the URL of the malicious applet. Do not forget to include **http://** before the address. Click **OK** to add the URL to the list.
5. AppletTrap will display the message "TO BE CALCULATED" until you click **Apply**. InterScan AppletTrap will check this site and then extract the hash code of the embedded applet.

Note: Hash codes are like fingerprints — once they are added to the list, InterScan AppletTrap will always identify the applets wherever they go; i.e., even if they move to other Web sites, the system will still recognize them.

---

6. Repeat the same procedure to add other malicious applets you know.
7. Click **Apply** to save the new list or **Cancel** to ignore the changes and load the previous settings.

Maintaining the InterScan AppletTrap & Internet Explorer Certificate Databases

As Java applets and ActiveX controls pass through the proxy server, InterScan AppletTrap runs a check on the certificates these mobile objects carry (i.e., if certificate checking is enabled)—comparing the certificates carried by applets with the system certificate database, and the certificates attached to ActiveX controls with the certificate database of Microsoft Internet Explorer.

Unsigned applets, those with unrecognized certificates, and those with certificates that do not match what is contained in the associated files are blocked and, in their place, InterScan AppletTrap creates a new applet that displays the following message when delivered to client workstations: **The applet is not properly signed and is blocked**.

In the case of ActiveX controls, the system replaces those not signed or carrying an unrecognized certificate with a new HTML page containing the message: **The URL <URL address> is blocked by InterScan AppletTrap**. This new page is then delivered to client workstations in place of the original page.

For information on how to enable certificate checking and how to specify a directory for saving ActiveX controls that have been blocked, please see the section "Configuring ActiveX Security" in Chapter 4, "Getting Started".

Maintaining the InterScan AppletTrap Certificate Database

InterScan AppletTrap keeps a database of recognized certificates that is automatically updated to include any new certificates encountered at the server. You can delete entries from this database and enable or disable entries.

InterScan AppletTrap complies with the CCITT X.509 international standard and only recognizes certificates that follow this standard. X.509 is the most widely accepted format for certificates and most, if not all, well-known Certifying Authorities (CAs) use this standard.

Note: After instrumentation, applets lose their original certificates due to code modification. InterScan AppletTrap, however, gives you the option to re-sign these applets using an imported "private key" so that they will be accepted by the clients' Web browsers.

How the System Uses the Java Applet Certificate Database

There are two sections in the certificate database of InterScan AppletTrap: the first section contains the names of the CAs, whereas the second contains the names of the publishers. To distinguish between CAs and publishers, please see the following:

- CAs issue certificates, publishers use these certificates to authenticate their software. One CA can have many publishers; for example, VeriSign, Inc.
- Publishers are software developers, CAs are not. For example, Trend Micro is a software developer.

When checking the certificate authenticity, InterScan AppletTrap uses the following algorithm:

1. Is the CA of that certificate recognized (i.e., included and enabled in the CA list of the database)?
2. Is the publisher of that certificate recognized (i.e., included and enabled in the publisher list)?

If both these conditions are met, the system passes on the applet. Otherwise, the applet is blocked. In the case of an unrecognized certificate, the system automatically imports it into the database, adding its CA name to the CA list and the publisher to the publisher list, if not yet included. Both entries, however, are disabled. InterScan AppletTrap then notifies the administrator and other designated recipients of this event.

Enabling/Disabling Entries

You can enable or disable entries in the system certificate database to selectively accept CAs and publishers at the server. Disabling a CA automatically disables all its publishers; disabling a publisher only affects that particular publisher — it neither affects its CA, nor the other publishers of the CA.

To enable or disable entries in the CA list...

1. From the left pane, expand **Java Applet Security** and **Certificates**.
2. Select **Certificate Authority**. The Certificate Authority page appears on the right pane. The check mark at the left of each entry signifies that InterScan AppletTrap currently recognizes that CA.
3. To enable a particular entry, select its corresponding checkbox. To disable, clear the checkbox. Click **Apply** to save the changes or **Cancel** to ignore the changes and load the previous settings

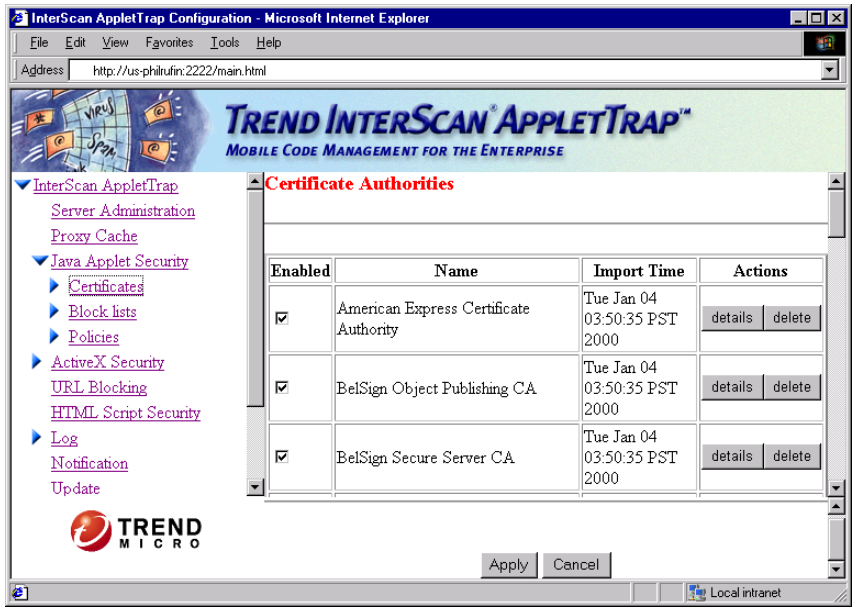


FIGURE 6-2. The Certificate Authority list.

To enable or disable entries in the publisher list...

1. From the left pane, expand **Java Applet Security** and **Certificates**.
2. Select **Commercial Publisher**. The Software Publishers page appears on the right pane.
3. To enable an entry, select its corresponding checkbox. To disable, clear the checkbox.
4. Click **Apply**.

Deleting Entries

You can delete entries from both sections of the database. Removing a CA does not affect any of its publishers already included in the list.

To delete a CA...

1. From the left pane, expand **Java Applet Security** and **Certificates**.
2. Select **Certificate Authority**.
3. Click on the corresponding **delete** button of the CA you want to remove.
4. Click **Apply**.

To remove a publisher...

1. From the left pane, expand **Java Applet Security** and **Certificates**.
2. Select **Commercial Publisher**.
3. Click on the corresponding **delete** button of the publisher you want to remove.
4. Click **Apply**.

Displaying Certificate Information

You can display information about a particular entry in the CA or publisher list, including the certificate's validity period, the issuing CA, and the publisher.

To display certificate information...

1. From the left pane, expand **Java Applet Security** and **Certificates**.
2. Select **Certificate Authority** or **Commercial Publisher**.
3. Click on the corresponding **details** button of the entry you want more information on.
4. Click **OK** to close the above screen.

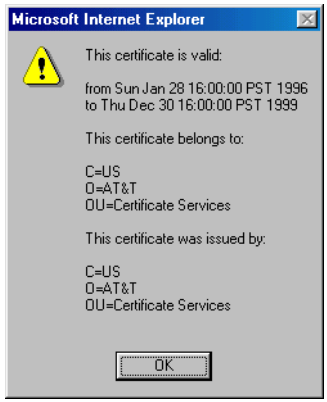


FIGURE 6-3. This screen displays information about a particular entry in the certificate database.

Importing a Java Applet Signing Key

InterScan AppletTrap can re-sign instrumented applets with your company's own "private key" before they are sent to client workstations. Since applets lose their original certificates during instrumentation, you may want to re-sign them to ensure that clients' Web browsers will always accept them without any restrictions.

To use the re-signing feature, you need two keys: 1) a "private key" that must be imported into the InterScan AppletTrap proxy server, and 2) the "public key" equivalent to your "private key" that must be imported into your clients' Web browsers. The "public key" enables the browsers to recognize the signature you affix to instrumented applets. Without this key, these applets will be treated as another unsigned applet — either blocked by the browser or given limited access to system resources.

InterScan AppletTrap supports the PKCS12 key format. If you already have a key but it is not in this format, you can use Netscape Communicator 4.04 (or later) to export it in the correct format. If you do not have a key yet, you can purchase one from any of the well-known Certifying Authorities (CAs).

If you do not have a key yet...

1. Open Netscape Communicator 4.04 (or later) and click the **Security** button on the Navigation Toolbar.
2. Under **Certificates** in the left pane, click **Yours**.
3. Click **Get a Certificate** and select the CA to connect to its Web site.
4. Follow the screen instructions to get your signing key. This key will be automatically imported into Netscape Communicator and will appear in the **These are your certificates** list box.
5. Select the imported key from the above list box and then click **Export**.
6. On the Password Entry Dialog screen, assign a password for your key and then confirm this password on the next screen.
7. On the File Name to Export screen, specify the complete path where you want to save your "private key." Make sure that **PKCS12 Files (*.p12)** is selected in the **Save as type** drop-down list box.

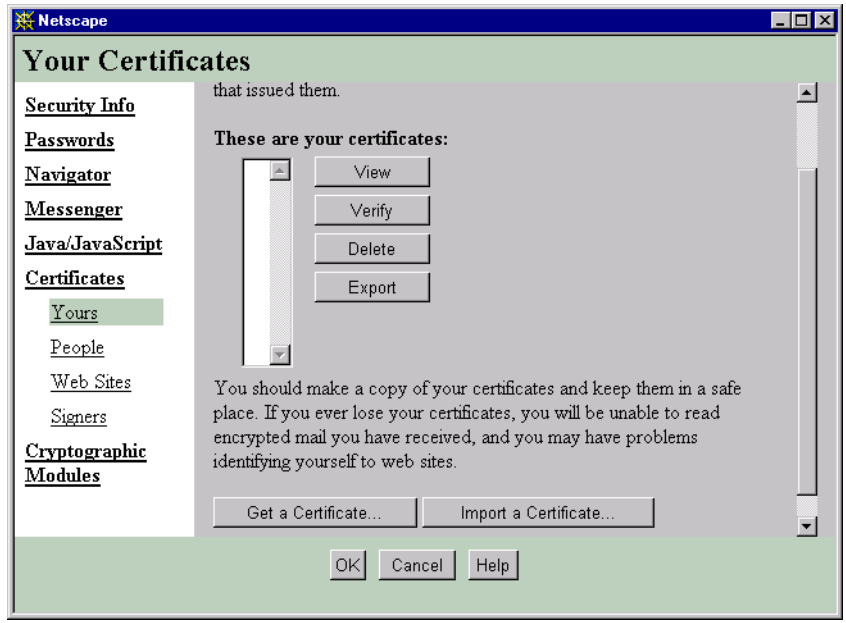


FIGURE 6-4. How to obtain CAs using Netscape Communicator 4.04 or later.

Importing a Key into InterScan AppletTrap

At any given time, only one key can exist inside InterScan AppletTrap — importing a new key automatically replaces the current one.

To import a signing key...

1. From the left pane, expand **Java Applet Security** and then **Certificates**.
2. Select **Signing key**. The configuration page for this option appears on the right pane.
3. Click **Import signing key**. Read and take note of the warning message.
4. Specify the complete path to your key in the **Select PKCS12 file** text box. Use the **Browse** button if needed.

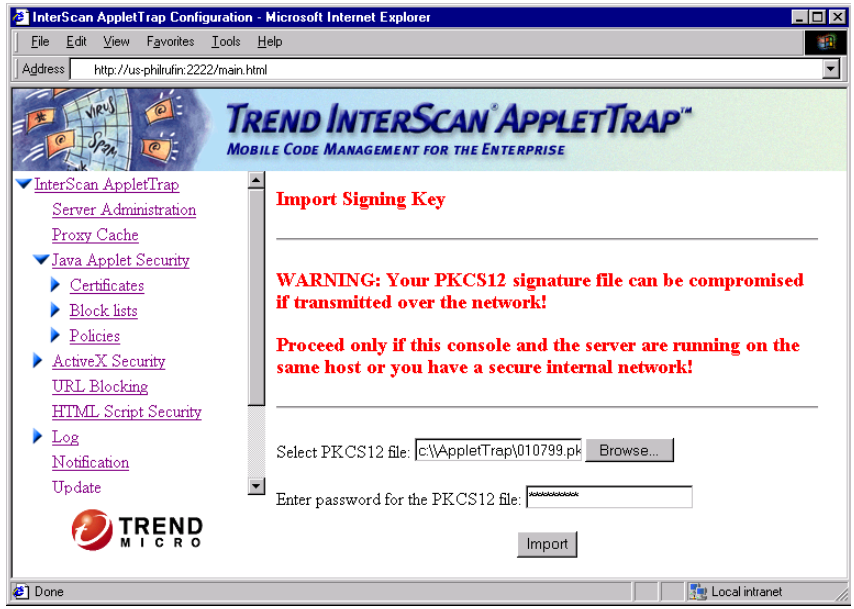


FIGURE 6-5. Importing a signing key (take note of the warning message).

5. Enter your key password in the provided text box. Then click **Import**.

6. The system notifies you that importation was successful by displaying the following message: **Successfully imported**.
7. Clicking **Signing Key** again displays a screen showing some information about your signing key.

Below is the list of all algorithms supported by AppletTrap:

- Message Digest: MD2, MD4, MD5, SHA1
- Symmetric-key Cipher: RC2, DES, 3DES, PBE/SHA1/3DES/CBC, PBE/SHA1/RC2/CBC
- Symmetric-key Cipher mode: ECB,CBC, CFB,OFB,PCBC
- Public-key Cipher: RSAEncryption
- Digital Signature: MD2withRSA, MD4with RSA, MD5withRSA, SHA1with RSA
- Others: PKCS7, PKCS8, PKCS12, X509

Importing a "Public Key" into Clients' Web Browsers

To ensure that your clients' Web browsers will always accept the instrumented applets re-signed by InterScan AppletTrap, perform one of the following:

- Import the "public key" equivalent to your signing key into their Web browsers
- Disable certificate verification on their browsers

If you do not have control over the Web browsers being used on your network, we recommend that you select the second option. If Netscape Communicator is the standard for your company, you can select either of the options above.

If you select the first option, Netscape Communicator will automatically import the "public key" attached to re-signed applets into the system database once granted permission by the user; i.e., when Netscape Communicator encounters a new signer, it prompts the user whether or not to accept it. Just instruct your clients to accept the new signature when prompted.

Note: The "public key" attached to re-signed applets is only specific to Netscape Communicator; other Web browsers such as Internet Explorer and Netscape Navigator will not recognize it.

If you select the second option, please refer to the documentation that came with the browser for information on how to modify its security settings.

Maintaining the ActiveX Certificate Database

InterScan AppletTrap uses the certificate database of Microsoft Internet Explorer to check for the authenticity of the certificates ActiveX controls carry. This database consists of three sections: the first section contains the personal certificates, the second contains the CAs, and the third contains the publishers. InterScan AppletTrap, however, only uses the last two sections in the filtering process due to security issues concerning personal certificates.

When checking the certificate authenticity of an ActiveX control, InterScan AppletTrap uses the following algorithm:

1. Is the CA of that certificate recognized (i.e., included and enabled in the CA list of the database)?
2. Is the publisher of that certificate recognized (i.e., included in the publisher list)?

If both these conditions are satisfied, the system passes on the HTML page containing the control to the intended recipients. Otherwise, a new page with a warning message is sent in place of the original page.

If so configured, InterScan AppletTrap also saves ActiveX controls into a specific directory at the server for later importation into the Internet Explorer's certificate database. To import a new certificate, you can either do it from within Internet Explorer or from the administrator console. One limitation of the latter method is that it can only modify the publisher list, whereas the former allows you to modify the entire database.

For information on how to specify a directory for saving ActiveX controls, please see the "Configuring ActiveX Security" section in Chapter 4, "Getting Started". For information on modifying the certificate database from within Internet Explorer, please refer to the Internet Explorer manual.

Modifying the Internet Explorer's Certificate Database from the Administrator Console

To modify the Internet Explorer's certificate database from the administrator console, you must access the console locally from the install machine and you must be logged on to Windows using the InterScan AppletTrap service account.

To modify the Internet Explorer certificate database...

1. Open the administrator console from the install machine.
2. From the left pane, select **ActiveX Security**. The ActiveX Security page appears on the right pane.
3. Click **Authenticode Validation**, then click **Manage Certificates**. InterScan AppletTrap accesses the publisher section of the certificate database and displays its contents in the list below.

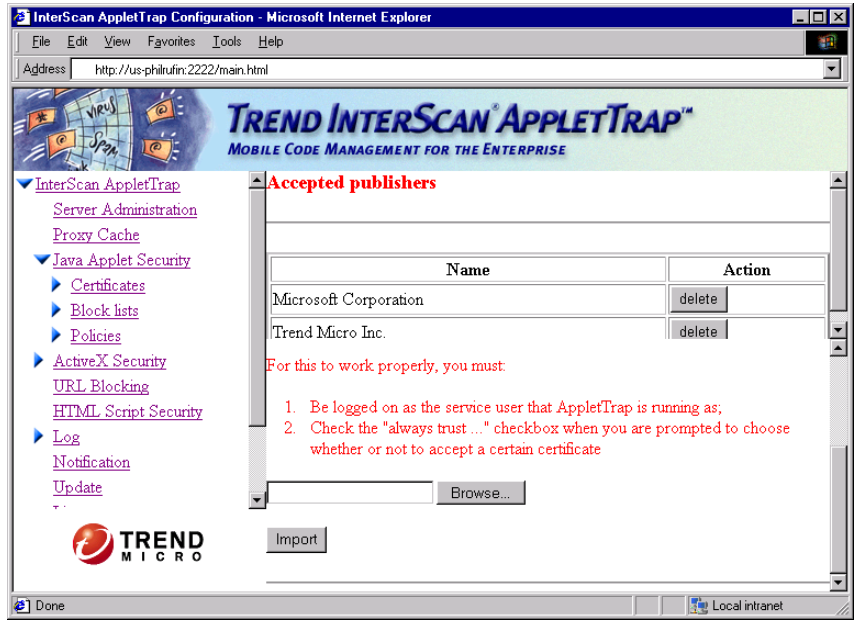


FIGURE 6-6. The screen for adding and removing publishers from the certificate database of Internet Explorer.

4. To add a new publisher, scroll down and specify in the provided text box the complete path to where its certificate is located. Use the **Browse** button if needed. ActiveX certificates are normally incorporated in CAB files.

   If you configured InterScan AppletTrap to save unrecognized certificates, you may be able to find those certificate files in the configured directory as well.

5. Click **Import**.

6. On the next screen, select the provided checkbox to always trust contents from the specified organization. Then click **Yes**.
7. Repeat the same procedure to add other publishers you want.
8. If you want to remove an entry from the list, click its corresponding **delete** button and then click **Apply**.

Note: The ActiveX authenticode feature only exists on the Microsoft Windows environment; and is not available on Solaris version. You need the Windows registry to get the ActiveX authenticode information.

Configuring Notification Messages

When malicious Java applets are detected on client workstations or when new entries are added to the system certificate database, InterScan AppletTrap can automatically alert, via email, the people you designate. For example, the administrator and other individuals who need to know when such events occur.

The email notifications contain customized text and some information about the event, such as the name of the new CA or publisher added to the database, the rule violated by the applet, its URL and hash code, and the IP address of the client workstation. Here are some sample notifications:

For malicious applets:

Found a malicious applet!

Reason: create new thread groups
URL: http://209.76.213.133/apptest/AppTest.jar
hostname: node3-205.javaapp.com
date: 10 Sep 2002 00:59:53 GMT
class:http://209.76.213.133/apptest/lib/ThrTest
Policyname: default
MD5-digest: 9MkXy2+6cKrLkcAf3fhrhQ==
ipaddr: 209.76.213.205

For new CA added to the database:

Certificate database has been updated!

New CA has been imported:
C=US

O=VeriSign, Inc.
OU=Class 3 Public Primary Certification Authority

For new publisher added to the database:

Certificate database has been updated!

New commercial publisher has been imported:
O=VeriSign Trust Network
OU=VeriSign, Inc.
OU=VeriSign Object Signing CA-Class 3 Organization
OU=www.veri-sign.com/CPS Incorp.by Ref.LIABILITY LTD.©97 VeriSign
OU=www.veri-sign.com/repository/CPS Incorp.by Ref.,LIAB.LTD©96
OU=Digital ID Class 3-Netscape Object Signing CN=Trend Micro, Inc.
L=Cupertino
SE
C=US

The first paragraph of the notification contains customized text. This is the only part of the message that is user-configurable—depending on the event that occurs, InterScan AppletTrap automatically fills in the rest. If you don't specify text for an event, InterScan AppletTrap will just send the event information minus the customized text to the recipient(s).

To configure notification messages...

1. From the left pane, select **Notification**.
2. Enter the name of the SMTP server on your network in the **SMTP server name** text box.
3. In the **Sender e-mail address** text box, specify the email address(es) to send notification to (usually the administrator).
4. In the **Recipients' e-mail addresses** text box, specify the email address(es) of the notification recipient(s). Use a comma to separate entries.
5. To enable notification for a blocked URL as it matches with any of the user-configurable list entries, select **Send notification when a URL is blocked due to Java/ActiveX hash or user defined URL**. Specify the message you want to include in the event information.
6. To enable notification for malicious applets, select the **Send notification when an instrumented applet violates a policy** checkbox. In the provided text box, specify the message you want included with the event information.

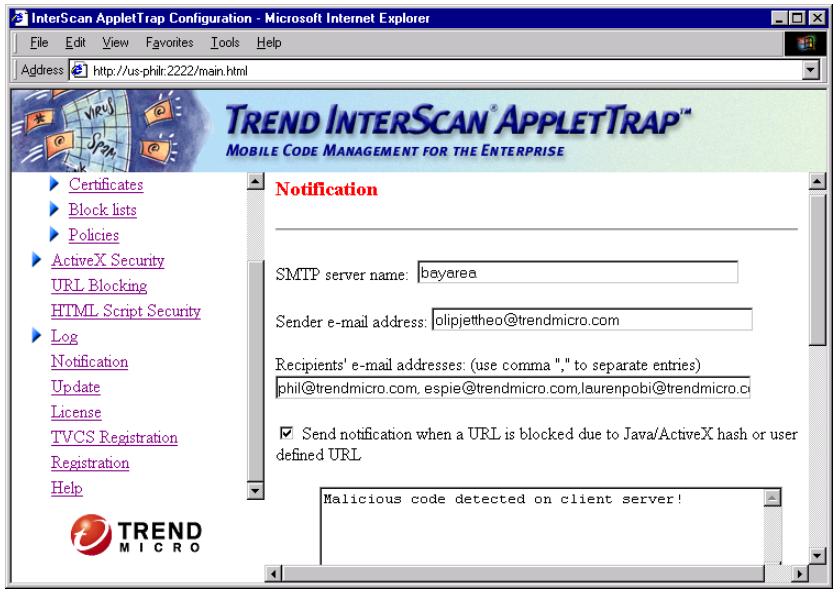


FIGURE 6-7. The Notification configuration screen.

7. To enable notification for database updates, select the **Send notification when new entries are added to the system's certificate database** checkbox. In the provided text box, specify the message you want included with the event information.
8. Scroll down and click **Apply** to save the changes or **Cancel** to ignore the changes and load the previous settings.

Chapter 7

Maintaining AppletTrap and Contacting Technical Support

This chapter contains information on:

- Displaying the Logs and Statistics
- Displaying debug messages
- Displaying performance statistics
- Deleting Log Files
- Product registration
- Uploading the user-configurable block lists to Trend Micro
- Updating the system block lists manually from Trend Micro
- Scheduling automatic block list updates
- Contacting Technical Support
- Virus Information Center
- SolutionBank Knowledge Base
- TrendLabs™

Displaying the Logs and Statistics

System Logs

InterScan AppletTrap keeps a running log of its activity. New logs are created daily and represent a valuable source of system information. You can examine all (or selected) log entries to learn details about the malicious applets, HTML scripts, and ActiveX controls detected at the server and on client workstations. In addition, you can view information about system status and operations.

There are two types of system logs:

- The **Mobile code log** contains information about the malicious mobile code detected by the system.
- The **Server log** records events related to system activities such as the status of each URL request, system startup, and system errors.
  If the display of debug messages is enabled, this log file will also include step-by-step information on how each URL request was processed—starting from the time that the client sends in the request until he/she gets a response. This information is particularly useful for diagnostic purposes. For information on how to enable this feature, please see the **Displaying Debug Messages** section.

The system keeps the log files in the **\LOG** directory of the InterScan AppletTrap install directory using the following file names: **applet.log.yyyy.mm.dd** and **server.log.yyyy.mm.dd** for the mobile code log and server log, respectively. **yyyy.mm.dd** displays the date when the log was created; e.g., **applet.log.2001.01.13** is the mobile code log for January 13, 2001. The log files are all in ASCII format.

To display entries in the mobile code log...

1. From the left pane, expand **Log** and then select **View Log**.
2. Select **View mobile code log**.
3. Under **Display Logs for**, select the option button for the log dates you want to view:
   - Select **All dates** to view the mobile code log for all the dates.
   - Select **Last 24 hours** to view the logs since midnight of the current day.
   - Select **Last 7 days** to view the logs generated over the past seven days.
   - Select **One month** to view the logs for the past 30 days.

- Select **A range** to view a range of dates. Specify the start and end dates for the log files you want to view.

4. Scroll down and click **View**.

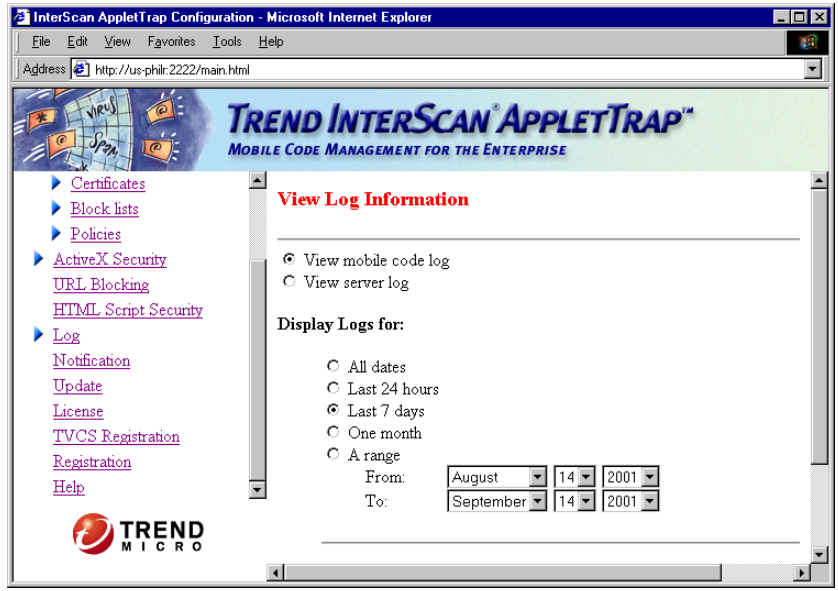


FIGURE 7-1. The screen for displaying entries in the log files.

To display entries in the server log...

1. Select **View server log** from the View Log Information screen.
2. Under **Display Logs for**, select the option button for the log dates you want to view:
   - Select **All dates** to view the server log for all the dates.
   - Select **Last 24 hours** to view the logs since midnight of the current day.
   - Select **Last 7 days** to view the logs generated over the past seven days.
   - Select **One month** to view the logs for the past 30 days.
   - Select **A range** to view a range of dates. Specify the start and end dates for the log files you want to view.
3. Click **View**.

Displaying Debug Messages

InterScan AppletTrap gives you the option to include debug messages, in addition to ordinary system messages, in the server log. These messages provide detailed information about the status of each HTTP request starting from the time that the client sends in the request up to the time he/she gets a response from InterScan AppletTrap.

If you want to closely monitor the InterScan AppletTrap operations, say for diagnostic purposes, enable this feature. Otherwise, disable this feature to minimize the size of the server log file. By default, this feature is disabled.

To enable display of debug messages...

1. From the left pane, select **Server Administration**. The Server Administration page appears on the right pane.
2. Select the **Include verbose messages in server log** checkbox.
3. Scroll down and click **Apply**.

FIGURE 7-2. Enabling display of debug messages (FireWall-1 version).

Displaying Performance Statistics

InterScan AppletTrap keeps two sets of counters for recording statistics related to the performance of the proxy server. The first set of counters records the current session starting from the time that the proxy server was started. The second set of counters records the entire history of the system (i.e., since installing the InterScan AppletTrap proxy server). Both counters provide information on the number of malicious applet attempts, applets blocked by URL, hash code and certificates, blocked ActiveX controls and JavaScript, total number of HTTP requests received, outstanding requests, and total number of instrumented applets.

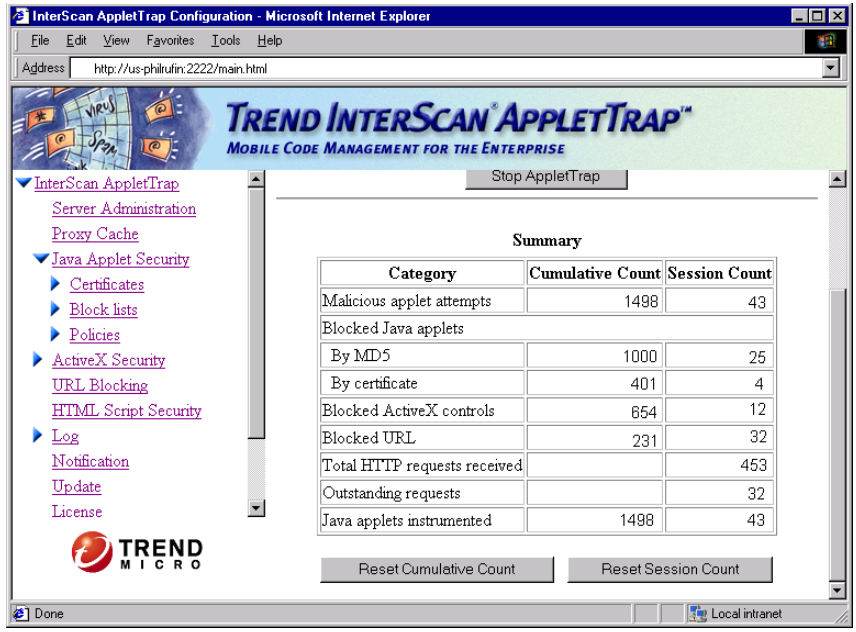


FIGURE 7-3. Cumulative Count displays the values for the entire history of the system, whereas Session Count displays the values for the current session (Standard version)

To view the performance statistics...

1. From the left pane, select **InterScan AppletTrap**.
2. Scroll the right pane to view the values.
3. To reset the counters for a specific group, click the appropriate reset (**Reset Cumulative Count** or **Reset Session Count**) button. Restarting InterScan AppletTrap also resets the session counters.

Deleting Log Files

Because InterScan AppletTrap creates and saves new log data every day, you may find that more logs have accumulated than you need. You can delete the excess log files manually or automatically.

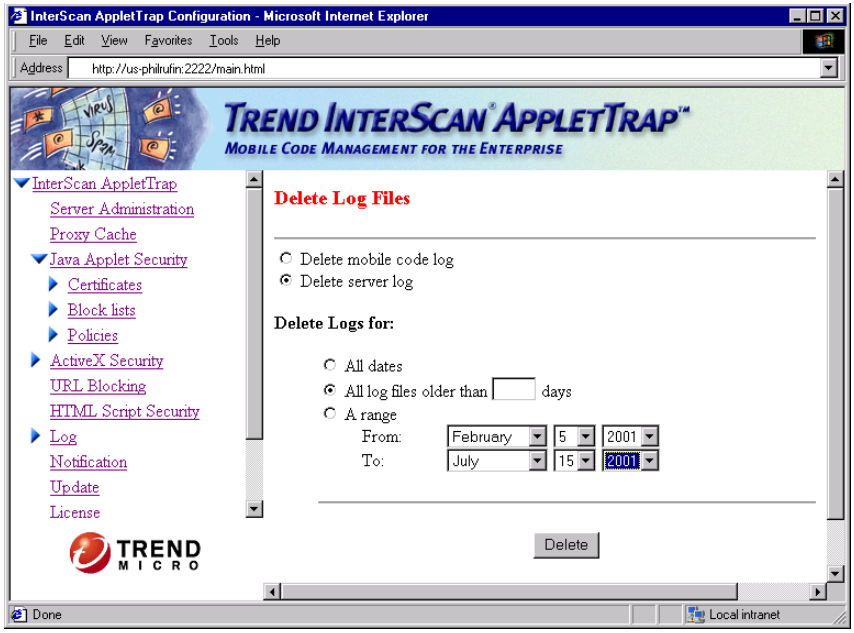


FIGURE 7-4. Deleting log files manually.

To manually delete log files...

1. From the left pane, click **Log** and then select **Delete Log**. The Delete Log Files page appears on the right pane.
2. Select the type of log file you want to delete using the radio buttons.
3. Under **Delete Logs for**, select the option button for the log dates you want to delete:
   - Select **All dates** to delete the logs for all the dates.
   - Select **All log files older than** to delete the logs older than the specified number of days. Specify the number of days you want in the provided text box.
   - Select **A range** to delete a range of dates. Specify the start and end dates for the log files you want to remove.
4. Click **Delete**.

To automatically delete log files...

This feature is disabled by default. To enable automatic log deletion,

1. From the left pane, click **Log** and then select **Schedule Auto Delete**. The Set Auto Delete Logs page appears on the right pane.
2. Select **Automatically delete all log files older than** and then specify how long you want to keep the log files in the provided text box. A setting of 3 days for example means that files older than 3 days will be deleted if they are left in the **\LOG** directory. Then click **Apply**.

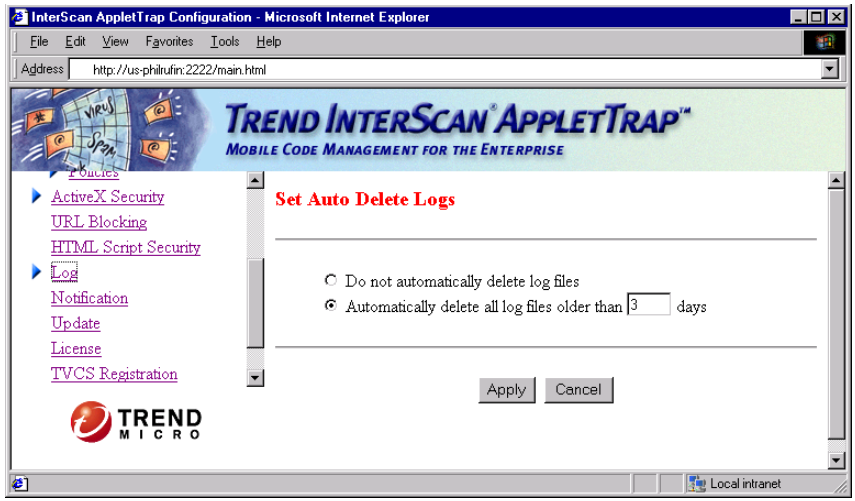


FIGURE 7-5. Scheduling automatic log file deletion.

Updating InterScan AppletTrap

Trend Micro provides a full year of free technical support and system block list updates to registered users worldwide. To take advantage of this benefit, please register your copy of InterScan AppletTrap with Trend Micro, as explained next in this chapter.

Once registered, you can choose to manually update InterScan AppletTrap or schedule automatic updates to occur at specific intervals. During updates, InterScan AppletTrap downloads the latest Java applet and ActiveX hash lists from Trend Micro's Web site onto your system, protecting it against the newest malicious activities. The update process also downloads the latest URL block list, updating the local copy to include all new entries found in the list kept at Trend Micro.

Trend Micro keeps its own hash list and URL block list at its site up-to-date by adding entries reported to us and those discovered by our engineers. In addition, during Internet updates, InterScan AppletTrap can be configured to automatically upload all the user-configurable lists to Trend Micro for verification. Any new entries found in these lists are analyzed and included in subsequent updates.

Registering InterScan AppletTrap

Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance.

Note: You must register online in order to automatically download updated block lists from Trend Micro.

To register online...

1. From the left pane, select **Registration**. InterScan AppletTrap connects to Trend Micro's Web site and displays the registration page.
2. Enter the requested information. Make sure to complete those text boxes with a red asterisk "*", which are required to submit the form.
3. Scroll down and click **Submit**.

To register by mail...

Fill out the self-addressed, stamped Registration Card included with the product

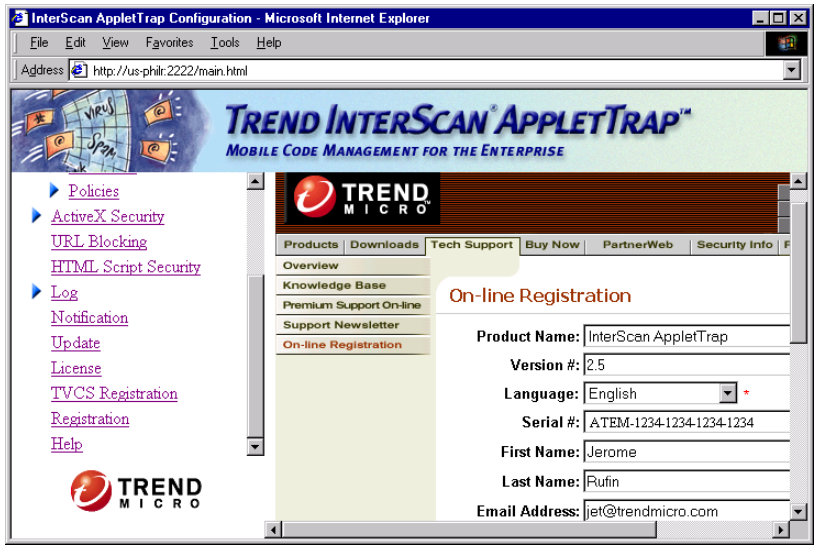


FIGURE 7-6. The registration form.

Uploading the User-Configurable Block Lists to Trend Micro

During Internet updates, InterScan AppletTrap can be configured to upload a copy of the user-configurable block lists to Trend Micro. These uploaded block lists will be given to Trend Micro's engineers for analysis. After a series of studies have been done on the instances of Java applets or ActiveX controls provided by customers, engineers will include those that are found to be malicious in the Trend Micro lists for future download.

By default, InterScan AppletTrap does not upload any of the user-configurable block lists to Trend Micro.

To upload the user-configurable block lists to Trend Micro...

1. From the left pane, select **Update**. The Update Block Lists page appears on the right pane:

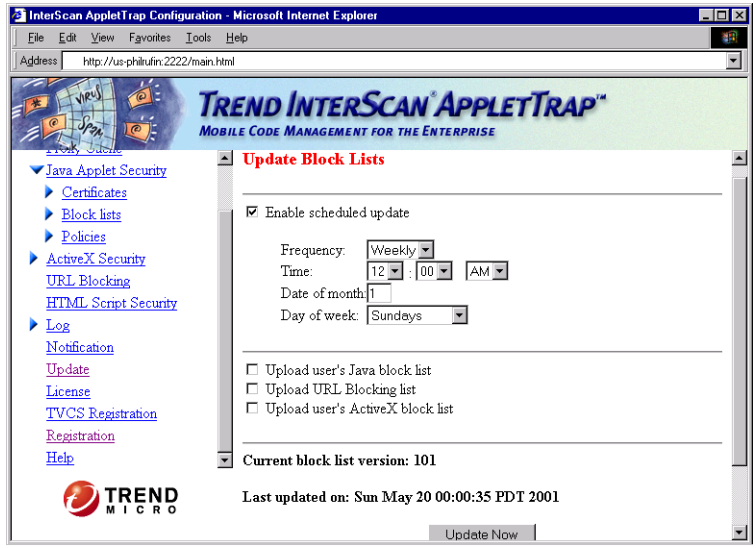


FIGURE 7-7. The configuration page for manually updating and scheduling Internet updates

2. To upload the user-configurable Java applet hash list, select the **Upload user's Java block list** checkbox.
3. To upload the URL list, select the **Upload URL Blocking list** checkbox.
4. To upload the user-configurable ActiveX hash list, select the **Upload user's ActiveX block list** checkbox.
5. Scroll down and click **Apply** to save the new configuration or **Cancel** to ignore the changes and use the previous settings.

Updating the System Block Lists Manually from Trend Micro

We recommend that you update your block lists at least weekly to keep up with the latest threats coming from malicious applets and ActiveX controls. Hundreds, and by some estimates, thousands of new malicious objects are written and released each year, so you should not allow your block lists to fall months out of date.

To update system block lists...

1. From the left pane, select **Update**. The configuration page for this option appears on the right pane.
2. Click **Update Now**.

InterScan AppletTrap updates the Trend Micro's block lists and, if configured to upload the user-configurable block lists, sends a copy of the block lists to Trend Micro for analysis. After successfully updating the downloadable block lists, InterScan AppletTrap displays the version and the current date of the new Trend's Hash list in the **Current block list version** and **Last updated on** fields, respectively.

Scheduling Automatic Block List Updates

To enable efficient use of your network bandwidth, we recommend that you schedule automatic updates to occur during weekends or in the wee hours of the morning when there are fewer users on the network.

To schedule automatic updates of Trend Micro's Block Lists (and upload the user-configurable block lists to Trend Micro if configured)...

1. From the left pane, select **Update**. The Update Block Lists page appears on the right pane:
2. Select the **Enable scheduled update** checkbox to enable this feature.
3. Select the update frequency from the **Frequency** drop-down list box. You have the option to update every day, once a week, or once a month.
4. Enter the time when you want the update to occur in the **Time** text boxes.

5. If you are updating once a month, enter the day of month in the **Date of month** text box. If you are updating once a week, select the day of week from the **Day of week** drop-down list box.
6. To upload the user-configurable Java applet hash list, select the **Upload user's Java block list** checkbox.
7. To upload the URL list, select the **Upload URL Blocking list** checkbox.
8. To upload the user-configurable ActiveX hash list, select the **Upload user's ActiveX block list** checkbox.
9. Scroll down and click **Apply** to save the new configuration or **Cancel** to ignore the changes and use the previous settings.

Contacting Technical Support

Trend Micro, Inc. provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all of our registered users.

- To view a list of the worldwide support offices, go to:
  `http://www.antivirus.com/support`
- To get the latest documents of every Trend Micro products, please go to:
  `http://www.antivirus.com/download/documentation/`

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

`http://www.antivirus.com`

`docs@trendmicro.com`

General US phone and fax numbers follow:

```
Toll free: +1-800-228-5651 (sales)
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
```

Please register your software before contacting our offices for support. Use any of the four easy ways to register:

- Register online from the program
- Register through the Web at:
  `http://www.antivirus.com/forms/register.htm`
- Fax the registration card to any Trend Micro office
- Mail the registration card to Trend Micro's US office

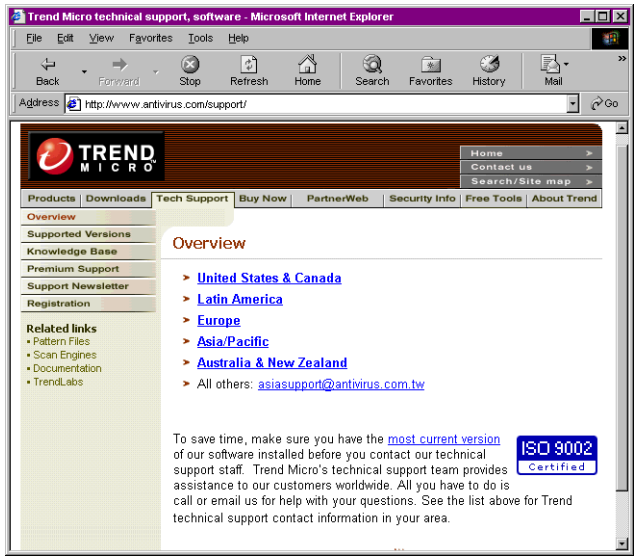


FIGURE 7-8. To obtain technical support, contact the Trend Micro facility nearest you.

Virus Information Center

Comprehensive security information is available on the InterScan WebProtect main window when you click the **Security Info** hyperlink at the top-right corner. You can also visit our free antivirus center at:

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

Use the Virus Information Center to find out about:

- Which viruses and malicious mobile code are currently "in the wild," or active

- Computer virus hoaxes
- A list of computer virus advisories
- Virus weekly report
- Trend Micro's Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Virus Primer
- Glossary of terms
- Safe Computing Guide

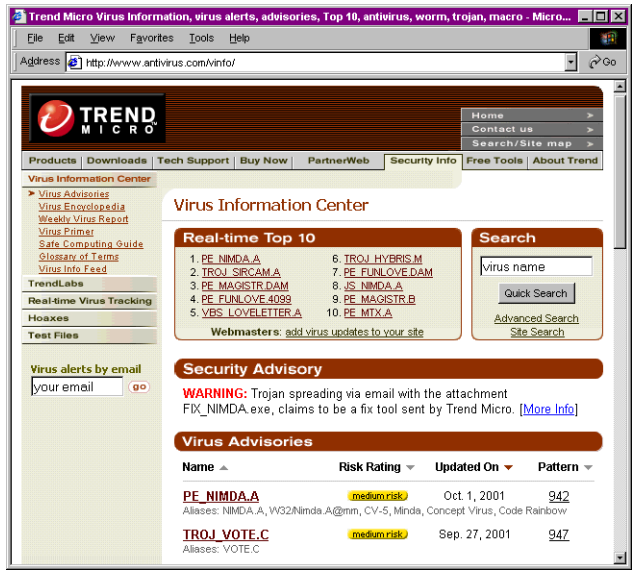


FIGURE 7-9. Trend Micro Virus Information Center.

SolutionBank Knowledge Base

The Trend Micro SolutionBank, maintained at the Trend Micro Web site, has the most up-to-date answers to product questions users have. You may also use SolutionBank to submit a question if you cannot find the answer in the product documentation.

SolutionBank is located at:

```
http://solutionbank.antivirus.com/solutions
```

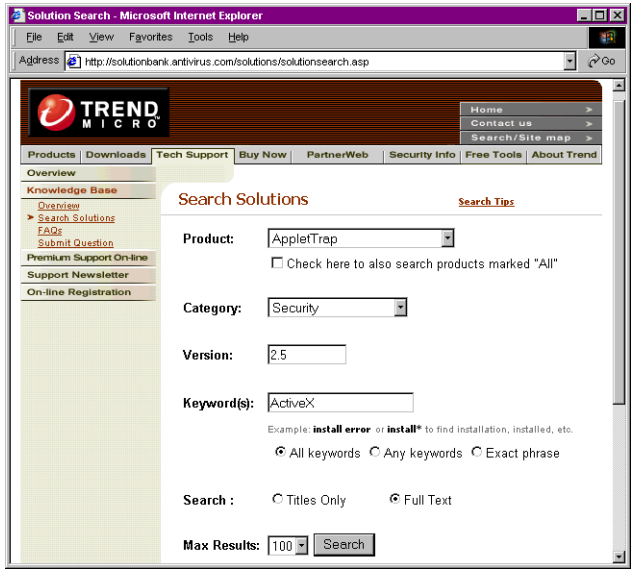


FIGURE 7-10. The contents of SolutionBank are being continuously updated, and new solutions are added daily.

The SolutionBank may be accessed using Internet Explorer, versions 4.0 or later, and Netscape Navigator, version 4.5 or later. Just sign up by entering your email address, name, phone number, and company.

Use SolutionBank, for example, if you are having trouble receiving Virus Pattern File updates and want to find out what you can do to solve the problem. As another example, say you're getting an error message--search SolutionBank using the text of message to find out what's causing the error and how to fix it. If you are unable to find an answer, however, you can describe the problem in email and send it directly to a Trend Micro support engineer who will investigate the issue and respond.

TrendLabs™

TrendLabs™ is Trend Micro's global complex of antivirus research and support centers. It's located on three continents, with a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

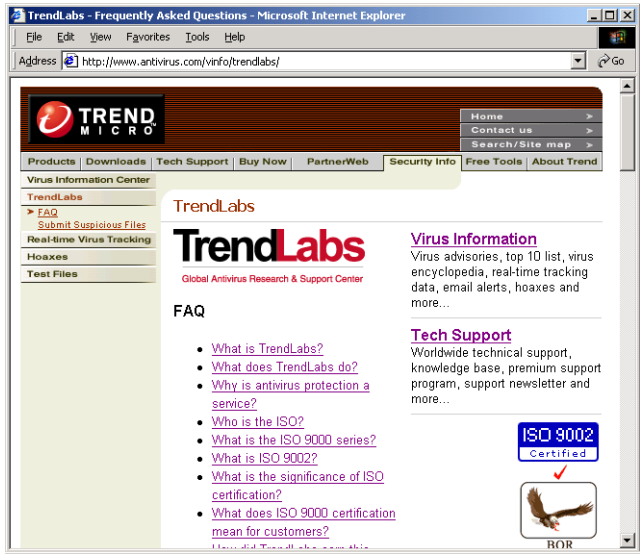


FIGURE 7-11. TrendLabs has achieved ISO 9002 quality assurance certification.

You can rely on the following post-sales service:

- Regular virus pattern updates for all known "zoo" and "in-the-wild" computer viruses and malicious codes
- Emergency virus outbreak support
- Free email access to antivirus engineers
- SolutionBank, Trend Micro's online database of technical support issues

.

Sending Trend Micro Your Viruses

If you have a file that is suspected to be infected with a virus but the scan engine does not detect it or cannot clean it, we encourage you to send the suspected file to TrendLabs at:

```
virus_doctor@trendmicro.com
```

Please include in the message text a brief description of the symptoms you are experiencing. Our team of virus engineers will “dissect” the file and remove any virus(es) it may contain. We will then return the cleaned file to you. Please visit the following site for information on "How to Submit Suspicious Files":

```
http://www.antivirus.com/vinfo/trendlabs/submit.htm
```

Index

R

S

T

U

V

W

Trend Micro Incorporated
10101 N. De Anza Blvd.
Cupertino, CA., 95014 USA
www.trendmicro.com

For Sales:
Tel: +1-800-228-5651 (US and Canada)
Tel: +1-408-257-1500 (outside US and Canada)
Fax: +1-408-257-2003

Item Code: ATEM20869/11005