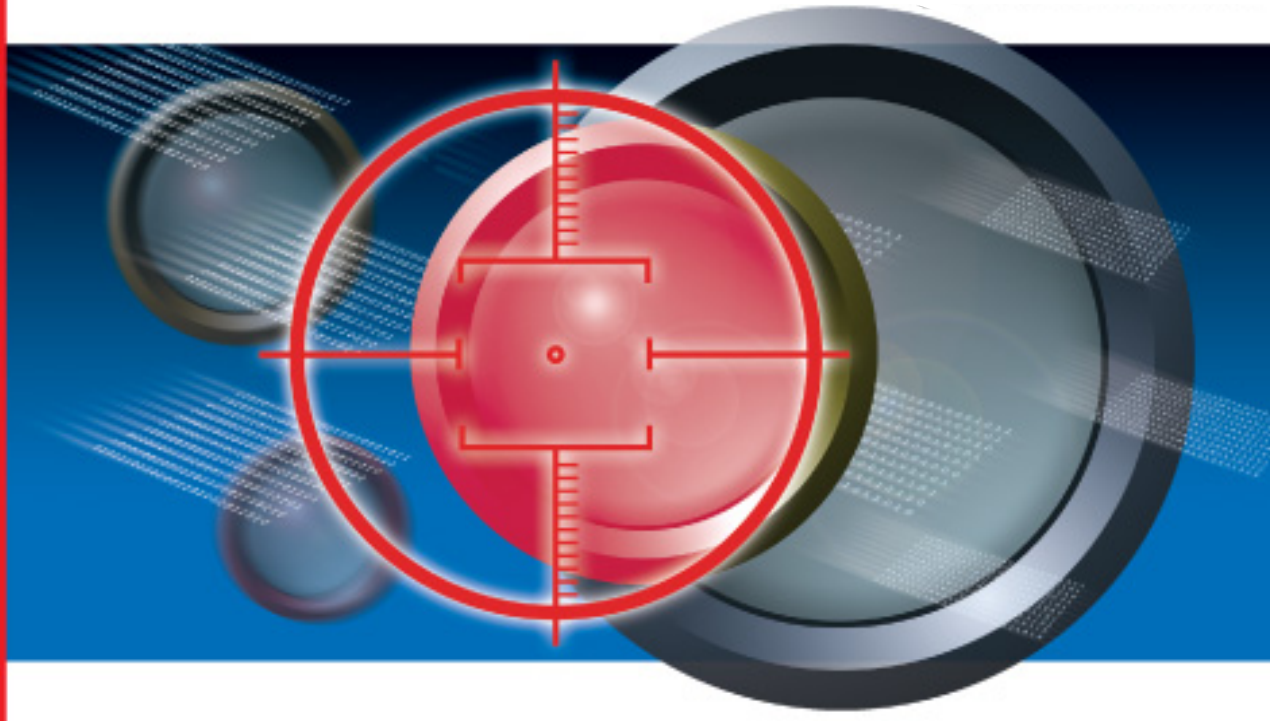
TREND MICRO™

Anti-Spyware Enterprise Edition 3.0

Enterprise-Class Protection, Enterprise-Class Management

for Windows™

Administrator's Guide



TREND MICRO™

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

http://www.trendmicro.com/download

NOTE: A license to Trend Micro™ Anti-Spyware Enterprise Edition software includes the right to receive pattern file updates, product updates, and technical support for one (1) year. Thereafter, you must renew Maintenance on an annual basis by paying Trend Micro's then-current Maintenance fees to have the right to continue receiving product updates, pattern updates and basic technical support.

Part number: ASEM32313/50620

Release Date: March 2006

The Administrator's Guide for Trend Micro™ Anti-Spyware Enterprise Edition is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

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

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

Table of Contents

Chapter 1

About Trend Micro Anti-Spyware Enterprise Edition

Trend Micro Anti-Spyware Enterprise Edition (ASEE) is a powerful tool for detecting and cleaning spyware on systems in your network environment. The product allows you to conduct a smooth, comprehensive desktop spyware protection rollout in very little time.

Understanding How Trend Micro Anti-Spyware Enterprise Edition Fits into Your Network

Trend Micro Anti-Spyware Enterprise Edition is based on a client/server model. The server provides policy and configuration settings, which software on the clients periodically polls. For the server to manage the clients, and for the clients to be able to poll the server for configuration, two-way communication must be possible between the server and the clients.

System Components

The following section outlines the main components of Trend Micro Anti-Spyware Enterprise Edition and their functions.

Enterprise Server

The Trend Micro Anti-Spyware Enterprise Edition server hosts the Web console and the server agent.

Web Console

The console provides a Web-based interface for administrators to manage the server and deploy and manage spyware protection throughout the network. You can choose to use Windows™ Internet Information Services (IIS) or Apache as the Web server, and can select either HTTP or HTTPS for connection.

From the console, you can easily deploy a scalable population of desktops. The Web-based console provides convenience and flexibility. This also allows access to network desktops through the variety of firewall configurations that might be deployed in your organization.

The Enterprise server is managed through the Web console. It can be configured to provide reports detailing scan/clean activity, listings of spyware found, network population, and other network security management parameters. Easy-to-navigate screens clearly show network status and options.

The (MySQL) Database resides on the server and holds information about the network's desktop population, configuration, desktop policy, and spyware found/cleaned feedback activity.

The Server Agent

The Server Agent, installed on the Enterprise server where Trend Micro Anti-Spyware Enterprise Edition is installed, provides communication between the server and Trend Micro's Spyware Research Center to check for spyware definition updates and product software updates. The Server Agent also handles communication between the Enterprise server and the network user desktops, for installation of updates throughout your network. The agent is designed so that user desktops do not require direct communication outside your network for updates.

The Anti-Spyware Agent

The Trend Micro Anti-Spyware Agent is a powerful desktop spyware detection and removal solution, proven over millions of installations. This agent communicates periodically with the Enterprise server to receive configuration and spyware definition database updates. The client also transmits client activity reports, via HTTP or HTTPS, back to the server. These reports include data on what spyware has been identified and cleaned, and current desktop configuration information.

Spyware Definitions

The spyware-definitions database is designed to accurately identify known spyware. Regular updates help minimize false positive notifications. In fact, many spyware signatures identified by other anti-spyware products are relatively harmless, yet they generate urgent notices and can create unnecessary concern for both administrators and users. These false positives can create havoc in the management process, burdening the network and server with extra traffic—exacerbating the problem that administrators are trying to defeat by installing the Anti-Spyware Software. False positives interfere with the ability to characterize actual spyware problems.

Active Monitoring

Integral to the capabilities of the Anti-Spyware Agent is Active Monitoring which proactively monitors file download and creation on the system to prevent new spyware infections. Active Monitoring includes Venus Spy Trap™ , a unique, real-time technology that proactively blocks “bad” ActiveX and other spyware programs by checking files against known spyware signatures

CWShredder™

Trend Micro Anti-Spyware Enterprise Edition also features CWShredder™, which eradicates the most difficult spyware, namely the variations around CoolWebSearch. The CoolWebSearch variants, known primarily for hijacking Web browsers, normally escape most other spyware detection products. However, with CWShredder, CoolWebSearch and its variants can be detected, cleaned and logged by Trend Micro Anti-Spyware Enterprise Edition.

Trickle Scan™

Traditional scanning methods can cause system slowdowns. Trickle Scan, a patent-pending technology, monitors CPU utilization of user applications during a scan, dynamically adjusts or "throttles back" scan-related CPU utilization if any increase in user application activity occurs, and resumes full scan CPU utilization when user activity drops. Benefits of Trickle Scan may include increased productivity and satisfaction, increased system performance during scans, and a reduction in help desk calls.

Trend Micro Anti-Spyware Enterprise Edition Functions and Benefits

Trend Micro Anti-Spyware Enterprise Edition provides powerful spyware detection and cleanup tools as well as remote management of desktop spyware protection. The solution provides a high-quality, relevant spyware-signature database and an efficient Trickle Scan™ feature that effectively balances end-user productivity and protection from spyware.

From the Web console, you can locate all desktops that are in Windows Networking domains through an automatic discovery process. As unprotected desktops are identified, the Server Agent module can be configured to automatically install the Anti-Spyware client, along with the Anti-Spyware signature database and the client agent, on each desktop. Desktop site visits by support staff are not necessary. From the console, you can also develop provisions to account for remotely deployed laptops or desktops for mobile workers.

During deployment, you can easily set a flexible range of policies (configuration settings) for desktops, or groups of desktops. Policies can follow the departmental organization, in which case there is a default automatic policy. Or, you can assign policies across domain lines, depending on user functions, responsibilities, or requirements. Typical policy parameters include scanning schedule, automatic installation and others. Policy options are covered in the *Setting and Using Policies* starting on page 24.

Chapter 2

Installing Trend Micro Anti-Spyware Enterprise Edition

This chapter outlines a step-by-step process for deploying Trend Micro Anti-Spyware Enterprise Edition on the server. It provides:

- Pre-installation information
- Server system requirements
- A walk-through of the product installation.

Note: Trend Micro suggests that you read through this entire section before beginning installation. Information on installing the client agent on remote computers is outlined in *Installing the Client Software* starting on page 36.

Pre-Installation Information

To prepare for the installation of Trend Micro™ Anti-Spyware, you will need to configure your firewall(s) and verify that the server, client desktops, and the network meet the configuration requirements outlined below. Once you have confirmed that your network and systems are correctly configured, proceed with the installation process. Trend Micro recommends reading through the entire Pre-Installation Information section before installing Trend Micro Anti-Spyware Enterprise Edition.

Connectivity and Network Rights

For the Trend Micro Anti-Spyware Enterprise Edition server to administer a desktop it must have TCP connectivity to the desktop. To automatically install a desktop, the server must have administrator rights for the domain to which the desktop belongs.

If this is not an option see *Installing the Client Software Using the MSI Installer* starting on page 41.

Note: A separate Trend Micro Anti-Spyware Enterprise Edition server is recommended for each distinct site in the organization.

Configuring Your Firewall

If a firewall is present in the intranet, configure it to allow network access to the following executables

On the server:

- tmassa.exe
- reminst.exe

On the client:

- tmasca.exe
- tmasea.exe
- imclntinst.exe
- ssapi32.dll
- cwshredder.dll

If you will be installing the client software on the Trend Micro Anti-Spyware Enterprise Edition server, configure your firewall to allow the server network access for all of the above executables.

Note: For client computers running Windows XP Service Pack 2 or Windows 2003 Server Service Pack 1, the internal firewall must be disabled or configured to allow connections required by Trend Micro Anti-Spyware. To configure the firewall, add the Apache web server port (default 8088), NetBIOS ports (137, 138, 139, 445), and socket mode using port (default 54447, 54448, or 54449) to your firewall exceptions. Consult your Windows help file for more information.

Minimum System Requirements: Server

Identify the Windows-based platform that is going to host the server. This server must not have an existing instance of MySQL. Trend Micro recommends that the server hosting the product have a static IP address rather than obtaining its IP address using DHCP.

The Trend Micro Anti-Spyware Enterprise Edition server software can be installed on a workstation or server that meets the following configuration requirements:

- Operating System:
  - Windows 2003 Standard and Enterprise with or without SP1
  - Windows 2000 Server and Advanced Server with SP4
- 256MB RAM
- 5GB disk space
- Internet Explorer 5.5 and above to access the Web-based user interface of the server

Note: Trend Micro Anti-Spyware Enterprise Edition requires a Java Virtual Machine (JVM) to display report graphics. At this time, only the Sun Microsystems™ JVM is supported.

Recommended System Configuration: Server

The following table provides server requirements information based on the number of clients that the server will manage.

Environment	Processor	RAM	Disk Space
Up to 12,500 clients	2.4GHz or faster	512MB	5GB
12,501 to 25,000	Dual 3.0GHz or faster	1GB	5GB
25,001 to 60,000 clients	Quad 3.4GHz or faster	2GB	5GB

Note: These recommendations are sufficient for the Trend Micro Anti-Spyware Enterprise Edition server software, database, and Web console components.

System Requirements: Clients

The client desktops in the network should meet the following configuration requirements:

- Windows 2003 Standard, Enterprise, and Web with or without SP1
- Windows XP Professional with SP1, SP2, or without SP
- Windows XP Home with SP1, SP2, or without SP
- Windows 2000 Server and Advanced Server with SP3 or SP4
- Windows 2000 Professional with SP3 or SP4

Note: For client computers running Windows XP Service Pack 2 or Windows 2003 Server Service Pack 1, the internal firewall must be disabled or configured to allow connections required by Trend Micro Anti-Spyware Enterprise Edition. To configure the firewall, add the Apache web server port (default 8088), NetBIOS ports (137, 138, 139, 445), and socket mode port (default 54447, 54448, or 54449) to your firewall exceptions. Consult your Windows help file for more information.

- 128MB RAM
- 10MB disk space

Installing the Server Software

From the host server, download the Trend Micro™ Anti-Spyware installation program from the Trend Micro Web site, or open it from the Trend Micro Installation CD. The installation file is `TMAS_EE.exe`.

Following the prompts from the Setup program, install the product on the designated platform. The installation will load, among other components, a Web server and MySQL databases to store configurations, desktop policies, and information about spyware detected and cleaned from the desktops.

Server Installation

To install the Trend Micro Anti-Spyware Enterprise Edition server software:

The installation program prompts you through the following steps:

1. Read and agree to the Trend Micro License Agreement by clicking **I Accept**.
2. Register Trend Micro Anti-Spyware Enterprise Edition.

   In order to activate Trend Micro Anti-Spyware Enterprise Edition, you need to enter a valid Activation Code. There are several ways to obtain an Activation Code:

   - As part of the product download
   - Through a reseller
   - Directly from the Trend Micro Web site

   Note: If you do not have an Activation Code, obtain one by registering your product. This can be done online through the Trend Micro Web site. You will need to enter your Registration Key (if applicable) and email address, along with additional registration information. Once you have completed the product registration process, you will receive an Activation Code by email.

   Click **Register Online** to register the product online and receive an Activation code via email then click **Next** to enter your Activation Code
3. Enter and confirm the administrator's email address for communications about spyware definition database updates and product updates from Trend Micro.
4. Select a destination directory (installation path) and click **Next**.

5. Set up the Domain Administrative account. Enter a user name and password that will be used to access workstations across the domain. This domain administrative account must have full Domain Administration rights for all domains that you will manage from the Web console. Click **Next** when done.
6. Select a user name and password for administrator access to the Web console and click **Next**.

Note: Be sure to record the IP address or host name of the server hosting the console. The IP address or host name is used to access the Web-based user interface to the server.

---

7. Configure the Web server connection:
   a. Select the port that Trend Micro Anti-Spyware Enterprise Edition will use for communication between the server and clients, and the Web console mode:
      - Windows™ Internet Information Services (IIS)
      - Apache
   b. Select **Use secure connection** to enable HTTPS for a secure connection to the Web console.
   c. Select a port for connecting to the Web console

      Note: The selected port must not be in use by any other Web server products.

   d. Click **Next**.
8. If your server has multiple IP addresses, select the IP address that you will use to access the Web console and click **Next**. The installation will load components, including:
   - The appropriate Web server component (IIS or Apache) and protocol (HTTP or HTTPS) for serving the Web console
   - A MySQL database to store information about configurations, desktop policies, and spyware detected and cleaned from the desktops.
   - A default policy for all discovered desktops in your network environment
9. When the final screen opens, click **Finish** to complete the installation process.

A Trend Micro Web console icon will appear on the Windows desktop of the server. Access the server Web console by clicking this link, to configure the policies and other settings of Trend Micro Anti-Spyware Enterprise Edition. You can also access the Web console remotely, by typing the IP address or host name and port number of the server in your Web browser.

Note: While you can access the console remotely, password changes can only be made when accessing the product locally.

For more information, see *Configuring the Trend Micro Anti-Spyware Server* starting on page 17.

Uninstalling the Server Software

If you need to uninstall the Trend Micro Anti-Spyware Enterprise Edition software from your server, use the Windows **Add/Remove Programs** tool.

To uninstall Trend Micro Anti-Spyware Enterprise Edition:

1. From the Windows **Start** menu, click **Settings** > **Control Panel**.
2. Select **Add/Remove Programs**.
3. From the list of currently installed programs, select **Trend Micro Anti-Spyware Enterprise Edition Server**.
4. Click **Change/Remove**.
5. Follow the prompts to uninstall Trend Micro Anti-Spyware Enterprise Edition.

Chapter 3

Configuring the Trend Micro Anti-Spyware Server

This chapter outlines a step-by-step process for configuring the Trend Micro Anti-Spyware Enterprise Edition server. You will access the Web console and set up your product with appropriate policies for your network environment.

Once the software is configured, see *Keeping Your Software Current* starting on page 21 for information on keeping your spyware definitions up to date, and *Managing Trend Micro Anti-Spyware Enterprise Edition* starting on page 51 for detailed information on using the product.

Starting Trend Micro Anti-Spyware Enterprise Edition

Trend Micro Anti-Spyware runs as a service under Windows, and will begin running as soon as installation is complete. While the product is active immediately after installation on the server, you must deploy the client software, create security policies for your network, and configure them to determine which computers on your network the policies apply to. Configuration is done via the Web console, which allows you to access the server remotely, from a computer in your network that is connected to the server via HTTP or HTTPS.

Accessing the Web Console

You can access the Web console by clicking the Trend Micro Anti-Spyware icon on Windows desktop if you are working directly on the server or have remote access to it. Alternately, type the IP address or hostname of the server hosting the Web console, followed by a colon and the connection port, to access the login screen.

For example: `http://127.0.0.0:8088`

If you selected **Use secure connection** to enable HTTPS, prefix the server address with HTTPS.

For example: `https://127.0.0.0:8088`

The **Summary** screen provides an overview of the status of Trend Micro Anti-Spyware Enterprise Edition, and provides a quick link to update anti-spyware definitions.

Logging Off the Web Console

To protect your installation of Trend Micro Anti-Spyware Enterprise Edition from unauthorized users, Trend Micro recommends logging off whenever you leave the computer where you are accessing the Web console. This helps prevent unauthorized access to the Web console.

To log off:

From any screen in the Web console, click the Log Off link in the upper right corner of the screen. This ends the current session and closes the browser window

Figure 3-1: The Log Off link

Using the Navigation Bar

The Trend Micro Anti-Spyware Enterprise Edition navigation bar is used to move between the Web console screens.

Figure 3-2: Navigation bar

You can also access the on-line help and Trend Micro support Web site from the navigation bar:

- Clicking on the navigation item opens the appropriate Web console screen:
  - **Summary**—shows overall status of Trend Micro Anti-Spyware Enterprise Edition
  - **My Enterprise Network**—shows all discovered desktops on the network
  - **Policies**—create, modify, and delete anti-spyware policies
  - **Reports**—provides access to reports and logs
  - **Administration**—common administrative tasks such as changing the Web console password, modifying the database, etc.
- Clicking **Help** opens the Trend Micro Anti-Spyware help file in a new browser window
- Clicking **Support** opens the Trend Micro Support Web site in a new window

Working with the Summary Screen

This screen displays the console summary information. The display includes the number of desktops discovered by the console upon installation. In this discovery process, the console reads the active directory list, which produces the initial **Total Desktops** entry. Any system connected to the network at the time will be included in the discovery process. The discovery process runs periodically, automatically reflecting changes in the network population.

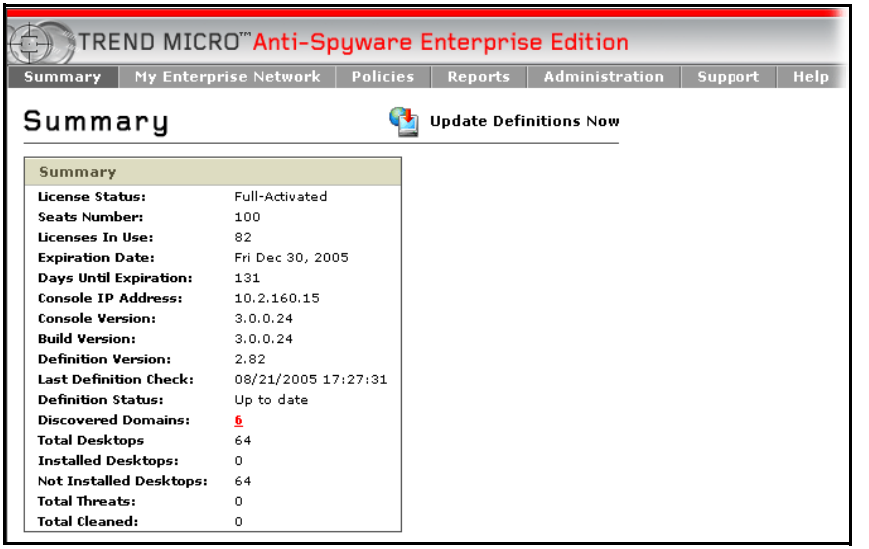


Figure 3-3: Summary screen

Understanding the Summary View

The information on the **Summary** screen is periodically updated to reflect current system data, including:

- Total Desktops
- Installed Desktops
- Not Installed Desktops
- Total Threats
- Total Cleaned.

The summary area also shows the console IP address, software version information, spyware definition version, and license information.

Note: If you log on the web console first time, you will see the **Domain Admin** page, you must active at least one domain, and then you can go to other pages. See *Chapter 4, Configuring Domains* for more information. For instructions on configuring proxy settings, see *Chapter 6, Changing the Proxy Settings*.

Keeping Your Software Current

Trend Micro Anti-Spyware Enterprise Edition detects spyware by comparing files on client computers with the spyware definition file. To maintain the highest level of protection against the spyware threats, you need to regularly update your Trend Micro Anti-Spyware definition file.

Updating Spyware Definitions

Trend Micro periodically issues spyware definition updates as new threats are identified. This helps to keep the spyware definitions current.

Updating Spyware Definitions on the Server

Trend Micro Anti-Spyware Enterprise Edition uses pattern-matching to locate spyware on computers where the client software is installed. To help ensure your

network is protected against spyware, Trend Micro recommends updating the spyware definitions regularly.

To update spyware definitions from the Summary screen:

1. Open the Web console.
2. Use the navigation bar to open the **Summary** screen.
3. Click **Update Definitions Now** in the upper right corner of the screen.

If the **Automatic Definition Update** setting for a policy is set to **On**, all desktops in the policy are updated with the latest version once it becomes available on the Trend Micro Anti-Spyware Enterprise Edition server.

Note: Trend Micro recommends configuring all policies to use **Automatic Definition Update** to ensure up-to-date protection for desktops in your network. For more information, see *Understanding Policy Settings* starting on page 25.

Updating Trend Micro Anti-Spyware Enterprise Edition

Trend Micro periodically updates the spyware definitions used by Trend Micro Anti-Spyware Enterprise Edition. Less frequently, the product itself is updated to take advantage of new engine technology or to improve scanning performance.

Trend Micro sends a notification to the email address used during product registration when updates are available for the Trend Micro Anti-Spyware Enterprise Edition application. Updates are distributed through a download from Trend Micro. All existing policy and desktop information is preserved after an update.

Chapter 4

Creating and Applying Policies

This chapter provides information on creating and using anti-spyware policies. Policy management is handled by the Web console, which provides access to the product interface from any computer on your network that has HTTP or HTTPS access to the server hosting it.

Information covered includes:

- Understanding policies
- Understanding the Global Default Policy
- Creating anti-spyware policies
- Modifying policies
- Assigning desktops to policy groups
- Understanding how network changes affect policies

Setting and Using Policies

An anti-spyware policy is a collection of configuration settings that control the scanning, cleaning, and active monitoring of a desktop. The **Policy** screen is used to create policies, select policy settings, and assign groups of client desktops to the policies.

Understanding the Global Default Policy

The global default policy is the policy that Trend Micro™ Anti-Spyware Enterprise Edition applies to desktops that are in administered (active) domains that do not have a specific policy applied to them. When the desktops are discovered, by default they are automatically added to the global default policy and the settings configured for that policy are applied to them. You can modify this policy, but it cannot be deleted.

Understanding Policy Options

You can modify the global default policy settings, add new policies, delete policies, and move groups of desktops into policies. You can control how desktops are grouped into policies. Policies can follow the departmental organization or emulate domain maps. Policy groups can also be assigned across domain lines, depending on user functions, responsibilities, or requirements.

Note: A client desktop can be a member of only one policy.

Understanding Policy Settings

The following policy settings control Trend Micro Anti-Spyware client activity on a desktop:

Setting	Explanation
Automatic Installation	When selected, all members of the policy automatically install the client software if their status is “Not Installed" or "Uninstalled".
Automatic Definition Updates	When selected, all members of the policy automatically update with new threat definitions as they become available.
Automatic Product Updates	When selected, all members of the policy automatically update with the newest version of the client software.
Active Application Monitoring	Enables monitoring by Venus Spy Trap™ (VST). VST monitors desktops to detect threats during file creation or execution. You can deny all spyware processes, allow all spyware processes, or present the user with a dialog and let him/her make the decision.
Scan Type	• **Full**—A full scan covers the entire disk and registry of a desktop. • **Quick**—The quick scan examines the common areas where security risks reside on the desktop.
Scan on Startup	When selected, the client runs a scan anytime the desktop is restarted.
Check Network Integrity	Enables protection of the desktop networking infrastructure. Sometimes removal of security risks can disable Internet/intranet access.
Automatic Cleaning	When selected, any security risks discovered during a scan are automatically cleaned.
Scan Schedule	Specifies the schedule of scans. Trend Micro™ Anti-Spyware Enterprise Edition automatically starts a scan at the specified day and time. Unless automatic cleaning is selected, this is a can only. To disable scheduled scanning, deselect all days.
Configuration Polling Interval	Specifies how often a desktop checks for Trend Micro Anti-Spyware policy changes. The value is in minutes.

Recommended Policy Settings

Trend Micro recommends configuring new policies as follows:

- Automatic Installation
- Automatic Definition Updates
- Active Process Monitoring
- Full Scan
- Scan on Startup
- Check Network Integrity

The choices for **Scan Schedule** and **Configuration Polling Interval** will depend on what is best for your network environment. Scanning every day provides optimal protection without any noticeable impact on the desktop user or the network. Configuration polling can be left at the default value.

Note: If automatic definition updates are not configured for the policy that the client belongs to, the client software will be installed with the spyware pattern that is packaged with the client installer. Trend Micro recommends manually updating the definition file for newly installed clients if you do not have automatic definition updates configured.

Creating New Spyware Policies

You may want to apply different policies to different desktops in your organization. To do this, you will need to create a policy other than the global default policy and apply it to those desktops.

To make a new policy:

1. Open the Web console.
2. Click **Policies** in the navigation bar.
3. Click **New Policy**.
4. The **New Policy Settings** screen opens.
5. Type the name of the new policy.
6. Configure the settings for the new policy. For detailed information on settings, see *Understanding Policy Settings* starting on Page 25.
7. Click **Save** to apply your changes to the policy.

Applying Policies to Policy Groups

The **Policy Screen** is used to build policy groups and perform operations on multiple desktops simultaneously. Individual members may be added or deleted according to parameters such as those outlined in *Understanding Policy Options* starting on page 24.

To apply policies to groups:

1. Open the Web console.
2. Click **Policies** in the navigation bar.
3. Click a policy name.
4. Click the **Policy Members** tab.
5. Click **Add members** to add new members to the policy.

Changing a Policy

You may need to make changes to existing policies as your network and security policy evolve.

To revise a policy:

1. Open the Web console.
2. Return to the **Policies** screen using the navigation bar.
3. Click the existing policy from the left column.
4. Click the **Policy Settings** tab.
5. Change the policy settings.
6. Click **Save** to apply changes.

Removing a Policy

You may want to remove a policy from your server.

To remove a policy:

1. Open the Web console.
2. Click **Policies** in the navigation bar.
3. Select an existing policy from the Policies list.
4. Click **Remove Policy**.

Note: Members of a removed policy are automatically re-assigned to the Global Default policy. They can be assigned to another existing policy if desired. Members can be moved from one policy group to another, by opening the new policy and adding a member from another group.

You cannot remove the Global Default policy.

Excluding Software from Cleaning

You may want to bypass removal of some previously identified security risks. This is accomplished by building an Exclude List.

To create an Exclude List:

1. Open the Web console.
2. Click **Policies** in the navigation bar.
3. Click a policy name.
4. Click the **Cleaning Options** tab.

5. To move a threat to the **Exclude List**, select it and click **Exclude**. Repeat for each source to be excluded.

   Note: You can select multiple sequential items by holding down the **Shift** key, or multiple non-sequential items by holding down the **Ctrl** key while selecting.

6. After you have finished selecting sources to exclude, click **Update List**.

To remove items from an Exclude List:

1. Open the Web console.
2. Click **Policies** in the navigation bar.
3. Click a policy name.
4. Click the **Cleaning Options** tab.
5. Select the item from **Excluded from Scan and Clean** list.

   Note: You can select multiple sequential items by holding down the **Shift** key, or multiple non-sequential items by holding down the **Ctrl** key while selecting.

6. Click **Include**.
7. Click **Update List**.

Configuring Domains

If you will be using domains to manage Trend Micro™ Anti-Spyware Enterprise Edition, you will need to select the domains that you will be managing. The server periodically scans the configured domains to find computers to manage. This process allows the server to automatically discover new clients on the network. Once you have configured a policy for a particular domain, you can configure Trend Micro Anti-Spyware to have computers that join that domain automatically download the client software

Discovered Domains

After installation, Trend Micro Anti-Spyware scans your network to discover available domains. These domains are added to the database of available domains which can be added to policies and used for management of your anti-spyware installations.

To view the discovered domains:

1. Open the Web console.
2. Use the navigation bar to open the **Administration** screen.
3. Click **Domain Admin** in the left panel.

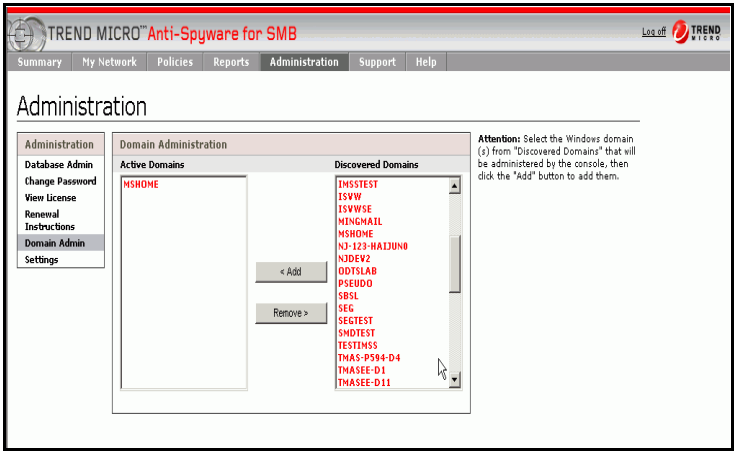


Figure 4-1: Domain Administration Screen

Administered (Active) Domains

Domains that are in the **Active Domains** list are available to policies. You can add or exclude domains from this list at any time

To include a domain in the Active Domains list:

1. Open the Web console.
2. Use the navigation bar to open the **Administration** screen.
3. Click **Domain Admin** in the left panel.

4. Select the domain(s) from the **Discovered Domains** list.
   You will see a list of domains that have been discovered.
5. Click **Add**.

Excluded Domains

Once you add a domain to the active domains list for management and machines are discovered and populated in the My Enterprise Network page, the machines are not automatically purged from the database when you go back and exclude the domain from management (discovery). Once a domain is excluded, Trend Micro™ Anti-Spyware Enterprise Edition no longer does discovery in that domain, but computers in that domain will still be displayed in the My Enterprise Network page and can still be managed. These computers can be removed by going to the Database Admin page and using the **Remove Domain** function.

Note: Before excluding a domain, you should first uninstall the client software from all computers in that domain. If you remove a domain from the "Active" list, installed clients on that domain will still be available through the My Enterprise Network screen.

To exclude a domain from the Active Domains list:

1. Open the Web console.
2. Use the navigation bar to open the **Administration** screen.
3. Click **Domain Admin** in the left panel.
4. Select the domain(s) from the **Active Domains** list.
5. Click **Remove**.

Note: Trend Micro™ Anti-Spyware Enterprise Edition will not attempt automatic discovery of new machines in domains in the Exclude list

---

Changes in the Client Network

If a new desktop is added to a domain, the periodic Trend Micro™ Anti-Spyware Enterprise Edition discovery process will identify the new client in the **Summary** screen as an uninstalled desktop and in the **My Enterprise Network** screen. The new desktop is automatically assigned to the global default policy (named Global_Default). The desktop should then be moved to another existing policy, or new policy, as needed.

Working With Remote Users

The administrator can also develop provisions to account for remotely deployed laptops or desktops for mobile workers. Before such a mobile or remote asset is issued to its user, it can be connected to the network and detected through the discovery process. This allows installation of the client agent, and subsequent updating and reporting upon reconnection to the network at a later time.

Once you install Trend Micro™ Anti-Spyware Enterprise Edition on remote user desktops and laptops, scanning and cleaning takes place in the background whenever they are used, as the client software applies the most recently loaded policy. The client software creates status information on the remote system. When these systems are logged into the network using a VPN, they become a part of the network, along with the desktops located in in-house domains. When they join a domain, these remote systems are automatically synchronized with the console for report results and updated with new spyware definitions as necessary.

When a Desktop Is Removed from a Domain

If a desktop is removed from the network, it is no longer detected by the discovery process. The information is deleted, and the desktop should be removed from the database from the **Database Admin** screen.

When a Desktop is Moved Between Domains

If a desktop moves from one domain to another, the transfer is automatically reflected in the My Enterprise Network screen by the periodic discovery process. Review the needs of that desktop in its new domain and revise the policies accordingly. The desktop will still exist in its old domain and you should remove the old entry to avoid confusion.

Chapter 5

Working with the Trend Micro Anti-Spyware Client Software

This chapter outlines a step-by-step process for installing Trend Micro Anti-Spyware Enterprise Edition client software. The client software performs spyware scanning on desktops and reports scanning and cleaning results to the Trend Micro Anti-Spyware Enterprise server.

Topics covered in this chapter include:

- Deploying the client from the console
- Manual installation
- Installing the client using the Microsoft Installer Service (MSI)
- Updating spyware definitions on the client

Installing the Client Software

There are two choices for installing the Trend Micro Anti-Spyware Enterprise Edition client software on computers:

1. If your network uses domains, you can install the client remotely using automatic or manual installation from the Web console.
2. If your network is not set up to use domains, you can install the client software using the client MSI installer. For more information, see *Installing the Client Software Using the MSI Installer* starting on page 41.

System Requirements for Clients

The client desktops in the network should meet the following configuration requirements:

- Windows 2003 Standard, Enterprise, and Web with or without SP1
- Windows XP Professional with SP1, SP2, or without SP
- Windows XP Home with SP1, SP2, or without SP
- Windows 2000 Server and Advanced Server with SP3 or SP4
- Windows 2000 Professional with SP3 or SP4

Note: For client computers running Windows XP Service Pack 2 or Windows 2003 Server Service Pack 1, the internal firewall must be disabled or configured to allow connections required by Trend Micro Anti-Spyware. To configure the firewall, add the Apache web server port (default 8088), NetBIOS ports (137, 138, 139, 445), and socket mode using port (default 54447, 54448, or 54449) to your firewall exceptions. Consult your Windows help file for more information.

- 128MB RAM
- 10MB disk space

Deploying the Client Software Using the Console

Clients are deployed in policy groups after the console has been installed on the management console server. The software can be deployed from the server to client machines either automatically or manually. In most instances, desktop clients will be members of policy groups that specify Automatic Installation.

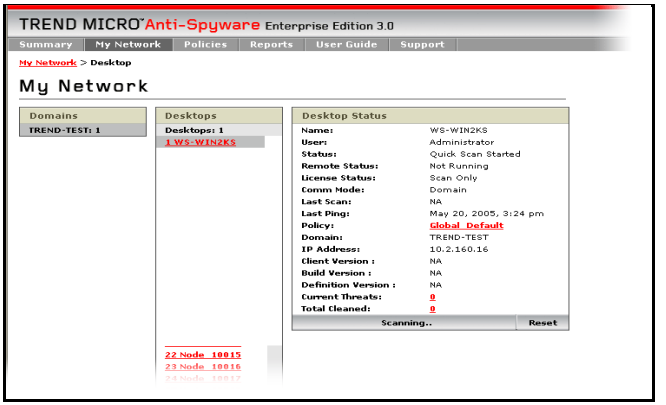


Figure 5-1: My Enterprise Network screen—desktop discovery

Note: The Anti-Spyware client software does not display a program icon in the client system tray. There are no controls available on the client.

For the console to administer a desktop it must have TCP connectivity to the desktop. For the console to automatically install the software into a desktop, it must have administrator rights for the domain the desktop belongs to. A server is recommended for each distinct site in the organization since these sites typically have different individual network administrators for each site.

Deploying the Client Using Automatic Installation

You can configure Trend Micro Anti-Spyware Enterprise Edition to install the Client Agent on all desktops in a particular domain automatically. This means that each new computer that joins the domain will automatically download and install the Client Agent.

To use automatic installation:

1. From the **My Enterprise Network** screen, confirm that all desktops have been discovered by the Enterprise server.
2. Click **Policies** in the navigation bar to open the **Policies** screen.

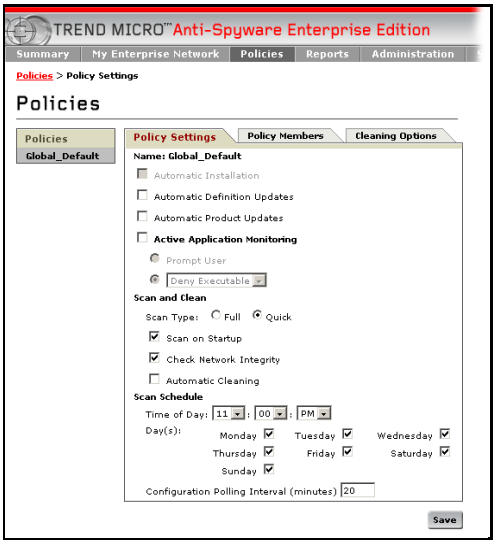


Figure 5-2: The Policies screen

3. Click the name of an existing policy to open the **Policy Settings** screen.
4. Click the **Policy Settings** tab.
5. Select **Automatic Installation** if it has not been selected for the new policy.
6. Click **Save**, and installation will begin immediately for that policy group.
7. Return to the **My Enterprise Network** Screen, and sort by Policy. The status for all desktops in the policy will change to "Installed."

8. The process is complete. All desktops added to the new policy are now being protected based upon the settings in the policy.

Note: If automatic definition updates are not configured for the policy that the client belongs to, the client software will be installed with the spyware pattern that is packaged with the client installer. Trend Micro recommends manually updating the definition file for newly installed clients if you do not have automatic definition updates configured.

Deploying the Client Using Manual Installation

You can manually install the Trend Micro Anti-Spyware Enterprise Edition Client Agent on all clients in a particular domain, or on selected desktops only.

To manually install client software:

1. From the Web console, click **My Enterprise Network** on the navigation bar.
2. Find the desktop in question by using the **My Enterprise Network** sort tool, sorting by domain or by policy.
3. Click on the name of the desktop where the agent will be installed, to open the **Desktop** screen.

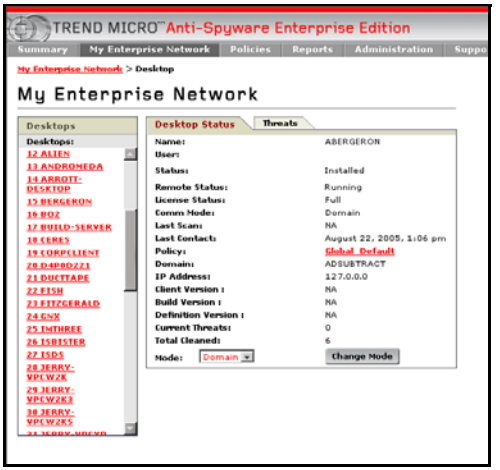


FIGURE 5-3. Desktop screen—Desktop Status tab

4. Click **Install**. The status for this desktop will change to "Installed."

Note: If automatic definition updates are not configured for the policy that the client belongs to, the client software will be installed with the spyware pattern that is packaged with the client installer. Trend Micro recommends manually updating the definition file for newly installed clients if you do not have automatic definition updates configured.

The status in the **Desktop Status** box reflects the current state of the desktop. When an installation is started, the status changes to "Installation in Progress." When the installation is complete, the status changes to "Installed."

Even before the first scheduled spyware scan, the installed Trend Micro Anti-Spyware desktop client immediately starts monitoring and blocking spyware program or file downloads, using the Venus SpyTrap™ capability if you have **Active Application Monitoring** enabled for the policy.

Tip: Trend Micro recommends running a test prior to installing groups of users by installing one desktop in each physical domain. This can be done using Manual Installation. The testing phase is a good time to check for infrastructure issues that might prevent proper operation. For more information, see *Connectivity and Network Rights* starting on page 8. Follow prudent rollout practice and install groups in order of mission priority or other sequence.

Installing the Client Software Using the MSI Installer

Trend Micro recommends deploying Trend Micro Anti-Spyware Enterprise Edition in the domain mode, when possible. In typical Windows networking environments, installing clients using this mode is the easiest. It also provides the greatest ease of management. For details, see *Deploying the Client Software Using the Console* starting on page 37.

Note: If you install the client software using the MSI installer, clients will not obtain licenses from the server. You need to add the license manually, or the client software will be configured to scan only.

For administrators who use a software distribution system to install and maintain software as needed, or for networking environments where domains are not used, Trend Micro recommends installing the client software using the MSI installer. The MSI installer has a lower bandwidth requirements than the domain installation.

If you are using a software distribution system, such as SMS or ZENworks® for Novell, you can run the MSI installation program remotely. If you do not have such a system and client computers on your network are not configured for remote management, you will need to run the installer on each individual computer.

Understanding Client Modes for Non-domain Environments

To operate Trend Micro Anti-Spyware in a network scenario where domains are not used, there are two options available:

- Socket mode—where all client/server operations are communicated through a socket connection
  There are three socket ports that may be specified: 54447, 54448, and 54449

  Note: You must have at least one of these ports available or you must specify a port. See the SERVERPORT section of *Understanding the Command Line Parameters* starting on page 43 for more information.

- Command polling mode—where the clients check for pending commands from the server at a specified frequency called the “Command polling interval.” This

mode enables client/server communication over HTTP or HTTPS, but is slower than socket mode.

Note: Either of these modes require the manual deployment of the client. The desktop client portion of Trend Micro Anti-Spyware Enterprise Edition can be deployed utilizing the client MSI (Microsoft Installer) installation tool.

If automatic definition updates are not configured for the policy that the client belongs to, the client software will be installed with the spyware pattern that is packaged with the client installer. Trend Micro recommends manually updating the definition file for newly installed clients if you do not have automatic definition updates configured.

Understanding the Trend Micro Anti-Spyware Enterprise Edition MSI Command Line Parameters

The following command line is used for manual deployment:

```
msiexec /i tmasclnt.msi ALLUSERS=1
RebootYesNo=No /Lve tmasclnt.log /qn SERVERIP=<Server IP
Address> SERVERPORT=<Non-standard port apache uses
(optional)> CMDMODE=<Command mode> SOCKET=<Non-standard
socket for client/server communication (optional)>
CMDINT=<Command Polling Interval (seconds)>
SERVERPROTOCOL=<Connection protocol>
```

Note: SERVERIP is a mandatory parameter. All others are optional.

Understanding the Command Line Parameters

The following section describes command line parameters and their values.

`/Lve <log file name>`

If you include this switch, an installation log file will be written to the computer where the client is installed.

Note: Trend Micro recommends using `tmasclnt.log` as a log name.

`/qn`

This switch selects “Quiet mode” which suppresses prompts for installation parameters. You must specify all required parameters to use the `/qn` switch.

`SERVERIP=<Server IP Address>`

This is a required parameter and identifies the IP Address to which all client-initiated communication will be addressed.

`SERVERPORT=<Non-standard port apache uses (optional)>`

This is an optional parameter which is used to tell the client that the Apache web server was installed on a port other than port 80. This parameter is only required if the Apache Web server on the server was configured to use a port other than port 80.

`CMDMODE=<Command Mode>`

This is an optional parameter that specifies the client/server communication method. One of three values can be selected:

- `CMDMODE=1`—indicates the client will be set in socket mode. In this mode, the client listens for communication from the server machine on one of three default socket ports for commands. If you set `CMDMODE=1`, you must specify a socket: `CMDMODE=1 SOCKET=xxx`

  Note: If you select this mode and choose a port other than one of the three defaults (54447, 54448, and 54449), you must configure all clients in the Network to use this same port. The Server Agent must be configured to use the same non-default port. Additionally, in this mode, Domain Mode clients cannot be switched to socket mode in the Web console. Configure the Server Agent using the /port switch.

  To resolve this problem, you must switch it back to Domain Mode or re-install this client using MSI command line and same non-default port.

  For example, from the Start menu, click run and type
  `X:\...\Anti-Spyware\tmassa.exe /port 54440`

- `CMDMODE=2`—indicates the client will be set in domain mode. In this mode, the client listens for communication from the server through the use of Administrative shares.
- `CMDMODE=3`—indicates the client will be set in command polling mode. In this mode, the client periodically polls the server to determine if there are any outstanding actions pending. If you set CMDMODE=3, you must specify a polling interval: `CMDMODE=3 CMDINT=xxx`

Note: If you do not specify a value for this option, the mode defaults to 1—socket mode.

SERVERPROTOCOL

This switch selects the connection protocol. Valid parameters are HTTP and HTTPS.

Note: If an invalid parameter is entered, the protocol will default to HTTP

Command Line Examples

For a new installation, use the following command structure:

```
msiexec /i tmasclnt.msi ALLUSERS=1 REBOOT=REALLYSUPPRESS
/Lve tmasclnt.log /qn SERVERIP=xxx.xxx.xxx.xx
SERVERPORT=x CMDMODE=x SOCKET=x CMDINT=x SERVERPROTOCOL=x
```

When installing over a previous version, where you do not want to uninstall, use the following command structure:

```
msiexec /i tmasclnt.msi REINSTALLMODE=vamus REINSTALL=ALL
ALLUSERS=1 REBOOT=REALLYSUPPRESS /Lve tmasclnt.log /qn
SERVERIP=xxx.xxx.xxx.xx SERVERPORT=x CMDMODE=x SOCKET=x
CMDINT=x SERVERPROTOCOL=x
```

Note: SERVERIP is a mandatory parameter. SERVERPORT, CMDMODE, CMDINT and SOCKET are optional.

Updating Definition Files on the Client

You can configure policies to automatically download the latest definition file from the server so that the client software always has the most current file available.

To update spyware definitions from the My Enterprise Network screen:

1. Open the Web console.
2. Use the navigation bar to open the **My Enterprise Network** screen.
3. Select the clients that you need update definition and click the **Update Definitions** button at the bottom of the screen.

You can also configure clients to download the latest version of the client software.For information on configuring policies for automatic definition updates, see *Understanding Policy Settings* starting on page 25.

Note: If automatic definition updates are not configured for the policy that the client belongs to, the client software will be installed with the spyware pattern that is packaged with the client installer. Trend Micro recommends manually updating the definition file for newly installed clients if you do not have automatic definition updates configured.

Uninstalling the Client Software

It may be necessary for you to remove a computer from your network, or to uninstall the client software. You can uninstall the client from a single desktop, or from multiple desktops.

Note: Uninstalling the client software from the Web console removes the license from use. Uninstalling the client software from the desktop itself using the Windows Add/Remove Programs will also remove the license from use, as long as the server is running and the client can connect to it.

Uninstalling the Client from One Desktop

To uninstall the client software from a desktop:

1. Open the Web console.
2. Click **My Enterprise Network** in the navigation bar.
3. Select the appropriate domain.
4. Locate and select the desktop to be uninstalled.

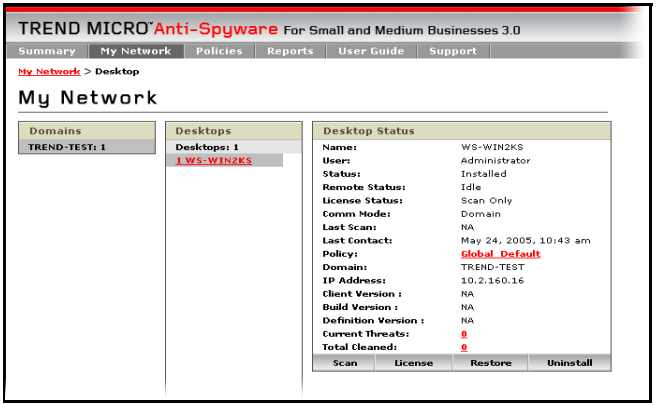


Figure 5-4: My Enterprise Network screen—uninstallation

5. In the **Desktop Status** box, click **Uninstall**.

Note: If the client software is uninstalled but the desktop is still part of your network, the desktop will still be recognized in the periodic discovery process. It will be listed on the **Summary** screen and **My Enterprise Network** screen and its status will be "Uninstalled."

Uninstalling the Client from Multiple Desktops

To uninstall the client software from multiple desktops:

1. Open the Web console.
2. Click **My Enterprise Network** in the navigation bar.
3. Select the desktops to uninstall.

   You can filter the view by domain, policy, or status.

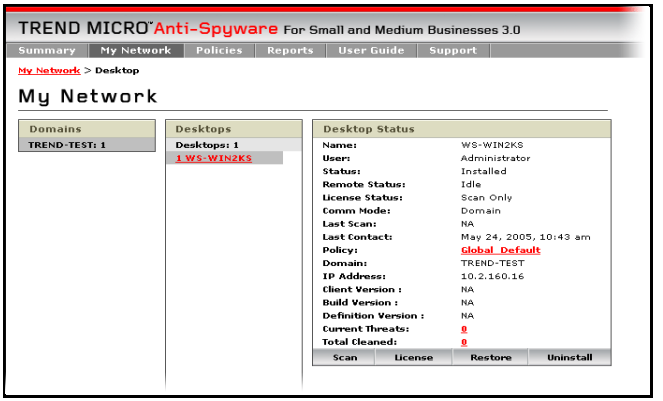


Figure 5-5: Uninstalling desktop software

4. Click **Uninstall** to remove the client software for all selected desktops.

Note: If the client is deleted, but the desktop is still part of your network, the desktop will still be recognized in the periodic discovery process. It will be listed on the **Summary** screen and **My Enterprise Network** screen and its status will be "Uninstalled."

Manually Uninstalling Client Software

You can use the Windows Add/Remove programs functionality to remove the Trend Micro Anti-Spyware Enterprise Edition client from a desktop.

Note: Uninstalling the client software from the Web console removes the license from use. Uninstalling the client software from the desktop itself using the Windows Add/Remove Programs will also remove the license from use, as long as the server is running and the client can connect to it.

Chapter 6

Managing Trend Micro Anti-Spyware Enterprise Edition

This chapter provides information on managing Trend Micro Anti-Spyware Enterprise Edition, including administrative tasks and spyware cleaning. Management is handled by the Web console, which provides access to the product interface from any computer on your network that has HTTP or HTTPS access to the server hosting it.

Information covered includes:

- Database management
- Setting the database properties
- Setting and changing passwords
- Mapping your network
- Scanning and cleaning desktops

Working with the Database

The **Database Administration** screen allows you to reset the **Total Threats** and/or **Total Cleaned** counts, remove a domain from the database, remove a desktop from the database, or administer the **Event Log** and **Cleaning History**.

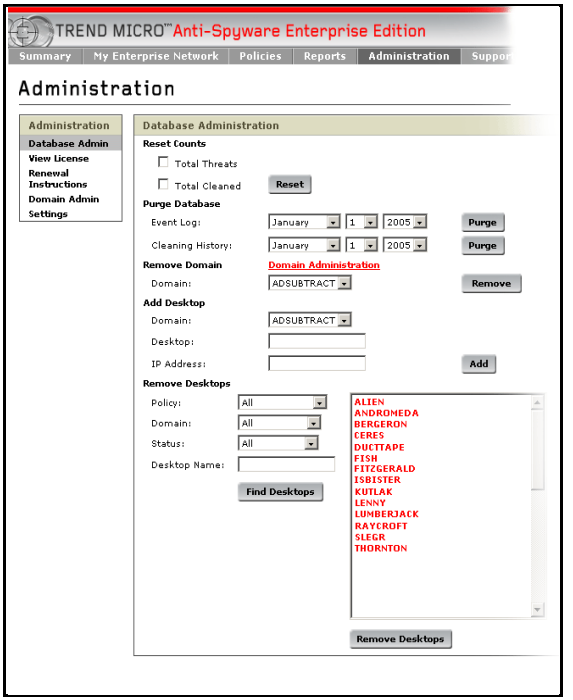


Figure 6-1: Administration screen—Database administration

To manage the database:

1. From the **Administration** screen, click **Database Admin**.

   The **Database Administration** screen opens, as shown in the previous figure.

2. Make any configuration changes:
   - **Reset Counts**—reset the threat and clean count to zero
     - **Total Threats**—select and click **Reset** to reset the threat count
     - **Total Cleaned**—select and click **Reset** to reset cleaned count
   - **Purge Database—**purge the database for:
     - **Event Log**—click **Purge** to delete items from the event logs prior to the date selected. A dialog "Proceed with Log purge" will display. Click Ok to purge the log.
     - **Cleaning History**—click **Purge** to delete items from the cleaning history prior to the date selected. A dialog "Proceed with Log purge" will display. Click Ok to purge the history.
   - **Remove Domain**—click **Remove** to remove a domain from the list of recognized domains

     Note: If you remove a domain from the database without uninstalling the client software all desktops in that domain will be removed from the My Enterprise Network screen. After the Configuration Polling Interval has elapsed, desktops with the client software installed will report back to the Enterprise server and will be populated into the My Enterprise Network with a status of Installed.

     Additionally, the domain will be removed from the "Active" list so no new discovery will be performed on that domain. The result is that only desktops with the client software installed in that domain will appear in the My Enterprise Network screen.

   - **Add Desktop**—allows you to manually add a desktop to the database by entering the desktop name or IP address

- **Remove Desktops**—allows you to manually remove a desktop from the database by selecting the desktop name or searching.
  - **Policy**—show only desktops in a particular policy
  - **Domain**—show only desktops in a particular domain
  - **Status**—show only desktops with a particular status

Note: If you remove a desktop from the database without uninstalling the client software and the desktop is in a domain that is "Active" (managed by Trend Micro™ Anti-Spyware Enterprise Edition), the desktop will be rediscovered and added back to the database during the periodic discovery process and its status will be **Installed**.

Setting the Database Properties

You can set the database properties of Trend Micro Anti-Spyware through the Web console. This allows you to configure the event log history, cleaning history, the My Enterprise Network refresh rate, and set the number of entries per page.

To set the database properties:

1. From the **Administration** screen, click **Settings**.
   The **Settings** screen opens.
2. Make any configuration changes:

- **Event Log History**—this value determines how long (in days) the event log will be kept in the database. Any event log that stays in the database longer than this value will be purged.
- **Cleaning History**—this value determines how long (in days) the records of cleaned spyware will be kept in the database. Any record that stays in the database longer than this value will be purged.
- **My Enterprise Network Refresh Rate**—the "My Enterprise Network" page presents the dynamic data from the database that shows all the desktops and domains. This page will be refreshed continually. This value determines the refresh interval (in minutes)

- **Set Entries Per Page**—some pages will list records in database (e.g., list of domains, desktops, and policy members). This value determines how many records will be displayed in one page.

Changing the Domain/Web Console Administrator User Name and Password

To help prevent unauthorized access to the Web console, you can change the administrator user name and password used to access the console. In many enterprises, the Domain Administrator user name and password must be changed periodically as a policy. To suit this requirement, you can also change the domain administrator user name and password that is used to manage the ASEE clients.

Trend Micro recommends choosing a hard-to-guess password and changing it periodically to help ensure Web console security. There are different ways to change the domain administrator user name and password depending on the Web server component you chose during installation (Apache or IIS).

Changing the Domain Administrator User Name and Password Under Apache

The domain user name and password are used to access the client machine when the server-to-client communication is in Domain mode. The server will use this account to copy file to the client machine and then start service on the client machine. This account should be a Windows domain administration account of the domains that you want to be managed by the Anti-Spyware server.

To change the domain administrator user name and password:

1. Open the Web console.

2. From the **Administration** screen, go to **Change Domain User Name and Password**.

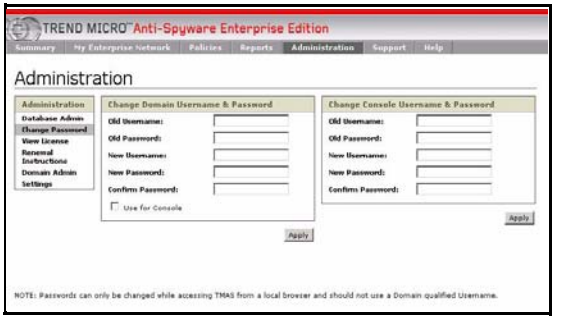


Figure 6-2: Administration screen—change password

Note: Note that there are two separate screens for **Domain** and **Console** user name/password management. You can also use the same user name and password for both domain and console by clicking the **Use for console** checkbox under the **Domain password management** screen.

---

3. Type the old user name and password.
4. Type and confirm the new user name and password.

Note: Passwords can contain alphanumeric characters (the letters a-z and the numbers 0-9) and punctuation. The double quote character (") cannot be used. The password cannot be blank, but can start with a space.

---

5. Click Apply.

Changing the Console Administrator User Name and Password Under IIS

You can change the domain or console's user name and password from the **Summary** screen.

Note: The console user name and password are used to access the Web console. The account is maintained by the Anti-Spyware server. This account does not need to be a Windows system account. You may use different user names and passwords for both domain and console. However, you can choose to use the same user name and password for both console and domain access.

You must access the Trend Micro Anti-Spyware Web console directly, rather than remotely, to change the domain and console user names and passwords.

Trend Micro recommends choosing a strong password and regularly changing it to protect access to the Web console. If you are using IIS, the Console user name/password management screen is displayed.

To change the Console administrator user name and password:

1. Open the Web console.
2. From the **Administration** screen, click **Change Password** in the left panel.

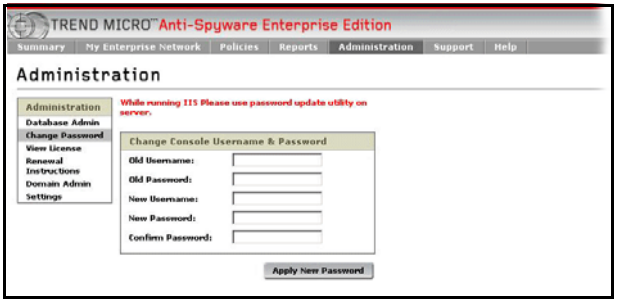


Figure 6-3: Administration screen—change password

3. Type the old user name and password.
4. Type the new user name and password.

5. Confirm the new password.

Note: Passwords can only contain alphanumeric characters: the letters a-z and the numbers 0-9. Special characters and punctuation (@, ", #, etc.) cannot be used. Password cannot be blank, and cannot start with a space.

6. Click **Apply New Password**.

Note: You must access the Trend Micro Anti-Spyware Web console directly, rather than remotely, to change the administrator password.

Changing the Domain Administrator User Name and Password Under IIS

If you are using Windows Internet Information Service to serve Web console pages from the server, you can change the domain user name and password using the password update utility. This utility must be run from the computer hosting the Trend Micro™ Anti-Spyware Enterprise Edition server software.

To change the console password, run the password update utility `aseepwd.exe`

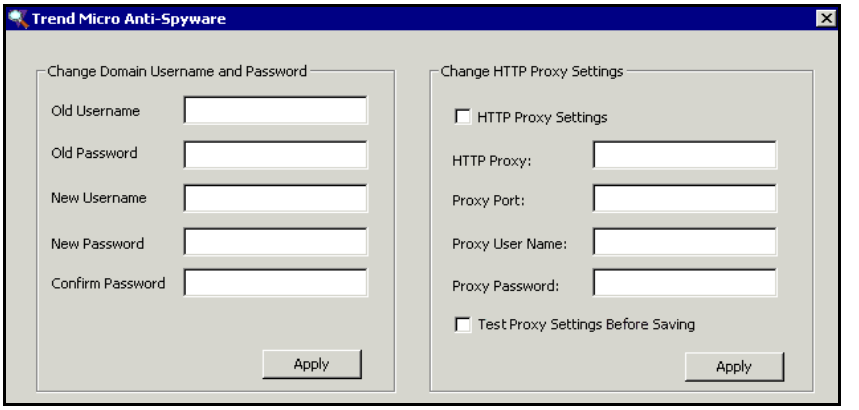


Figure 6-4: Password Update Utility

To change the Domain Administrator user name and password:

1. Run the password update utility `aseepwd.exe` from the Windows **Start** menu or the Trend Micro™ Anti-Spyware Enterprise Edition installation directory.
2. Type the old user name and password.
3. Type and confirm the new user name and password.
4. Click **Apply**.

Changing the Proxy Settings

To ensure that your server has the latest spyware definition files available, it must be able to connect to the Internet to download the latest definitions from the Trend Micro ActiveUpdate servers.

Changing the Proxy Settings for Apache

If you chose the Apache server as your web server, you must change the proxy settings via the Web console.

To change the proxy settings in Apache:

1. Open the Web console.
2. Open the **Proxy Settings** screen by clicking **Administration** in the navigation bar and selecting **Settings** in the left panel.

Figure 6-5: Settings screen for Apache

3. Make the appropriate changes to your proxy settings.
4. Click **Save**.

Changing the Proxy Settings for IIS

If you chose the IIS server as your web server, you will need to run the password update utility `aseepwd.exe` to change the proxy settings.

To change the proxy settings in IIS:

1. Run the password update utility `aseepwd.exe` from the Windows Start menu by clicking **Start** > **Programs** > **Trend Micro Anti-Spyware Enterprise Edition** > **Trend Micro Anti-Spyware Password Utility** or open the program directly from the Trend Micro™ Anti-Spyware Enterprise Edition installation directory.

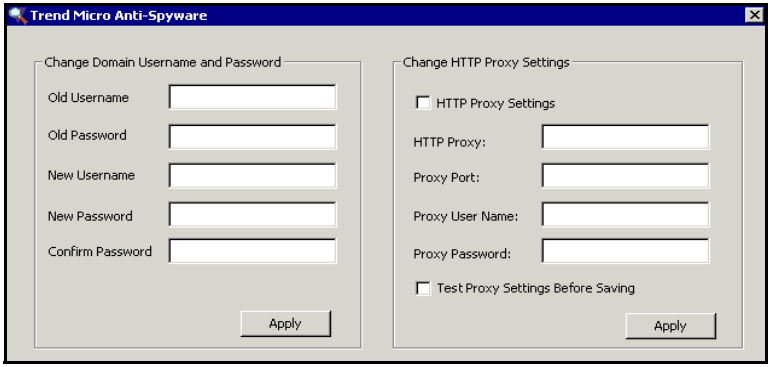


Figure 6-6: Settings screen for IIS

2. Make the appropriate changes to your proxy settings.

Note: You can select **Test Proxy Settings Before Saving** to perform a proxy settings check. If the check fails the proxy settings may need to be changed, or Trend Micro™ Anti-Spyware Enterprise Edition may simply be unable to verify the settings. If your proxy server is not configured to allow Trend Micro™ Anti-Spyware Enterprise Edition server to connect to itself, deselect **Test Proxy Settings Before Saving**.

3. Click **Apply**.

License Renewal

To renew your Trend Micro™ Anti-Spyware Enterprise Edition license after it expires, you need to obtain a new Registration Key through your reseller or the Trend Micro organization responsible for maintenance renewals and a new Activation Code. Once you receive your new renewal Registration Key, you can obtain a new Activation Code online through the Trend Micro Web site.

Note: You will need to enter your Registration Key and email address, along with additional registration information. Once you have completed the product re-registration process, you will receive an Activation Code by email.

You can view the status of your product license from the **Summary** screen. Follow the directions below to enter a new Activation Code from the **Administration** screen.

To enter a new Activation Code:

1. Open the Web console.
2. Open the license screen by clicking **Administration** on the navigation bar, then clicking **View License** to open the License page.
3. Click the **Enter a new code** link.
4. Type your Activation Code in the field.
5. Click **Activate**.

Scanning and Cleaning Desktops

The following section explains how to scan desktops for spyware and clean them. The two modes of operation for scanning and cleaning are automatic and manual.

Scanning and Cleaning Automatically

Once policies are created and the client is installed, desktop scanning occurs automatically according to the scan schedule. No further intervention by the network administrator is required. If automatic cleaning is selected in the policy setting, Trend Micro™ Anti-Spyware Enterprise Edition eliminates all spyware identified in the scan with no further intervention. Information on scan and clean results is available through the reports. (See *Working with Reports* starting on page 67 for more information).

Scanning and Cleaning Manually

There may be instances where a desktop might need to be scanned or cleaned manually. Scans and cleans of individual desktops can be initiated at any time.

To manually clean a desktop:

1. Open the Web console.
2. Click **My Enterprise Network** on the navigation bar.
3. Sort by Domain or Policy to find the desktop in question.
4. Click on the name of the desktop to be scanned.

Note: You can scan multiple desktops by selecting them and clicking the scan button.

---

5. Click **Scan** in the **Desktop Status** box.

Note: The remote status changes to "Scan in Progress" when a scan is started. When the scan is complete, the status changes to **"**Idle".

---

6. To view threats, click the threat count in the **Desktop Status** box. This opens the **Threats** box showing all the threats identified on that desktop.
7. To clean threats discovered on this computer, click **Clean All Threats**.

Restoring Desktop Software

There may be times when you need to restore a cleaned application to a desktop. In cases when you need to restore deleted or cleaned suspect spyware files, Trend Micro Anti-Spyware stores up to 15 of the most recent cleans, which can be restored using the **Restore** button in the management console.

To restore recent occurrences of cleaned threats on a desktop:

1. Open the Web console.
2. Click **My Enterprise Network** on the navigation bar.
3. Either:
   a. Select a desktop
   b. Click **Restore to Last Point**

   or

   a. Under **Desktops**, select the name of desktop in question.
   This will open the **Desktop** screen to the **Desktop Status** tab.
   b. Click **Restore**.
   c. The **Restore** screen opens, showing recent cleanings for that desktop.
   d. Select a clean point and click **Restore**.
   The items included in the selected clean points will be restored.

Note: The maximum number of restore logs is fifteen. After fifteen restore logs have been written, future logs overwrite existing logs on a first-in, first-out basis.

Chapter 7

Working with Logs and Reports

This chapter provides information on using Trend Micro™ Anti-Spyware Enterprise Edition logs and reports. Management of these tasks is handled by the Web console, which provides access to the product interface from any computer on your network that has HTTP or HTTPS access to the server hosting it.

Information covered includes:

- Viewing the Event Log
- Working with reports

Viewing the Event Log

The Event Log maintains a record of all desktop activities related to Trend Micro™ Anti-Spyware Enterprise Edition. A history of all scans, cleanings, restores and other activities is included in the event log.

For each event, the Event Log shows:

- Date-Time
- Event Type
- Category
- Domain
- Desktop

For more detailed information about an event, click anywhere on the event log line for that event. This can be particularly useful in determining trends and troubleshooting problems. Using the **Power Search** button on the **Reports** screen, the network administrator can create a range of management reports sorted by event type, domain, desktop, or category.

Working with Reports

Trend Micro™ Anti-Spyware Enterprise Edition provides reporting functions that allow you to monitor the state of the clients on your network and to understand how prevalent threats are on those clients. Reports are available for viewing through the Web console and in a version for printing. The use of a MySQL database permits numerous query possibilities, resulting in a choice of reports to help the network administrator stay abreast of threats and other network spyware protection activity.

Note: The reporting pages require that you have Java enabled for your browser. The latest Java Runtime Environment (JRE) can be found at http://java.sun.com. Trend Micro™ Anti-Spyware Enterprise Edition does not support the Microsoft Java Virtual Machine.

To view reports:

1. From the Web console, click **Reports**.
2. Choose the type of report to view

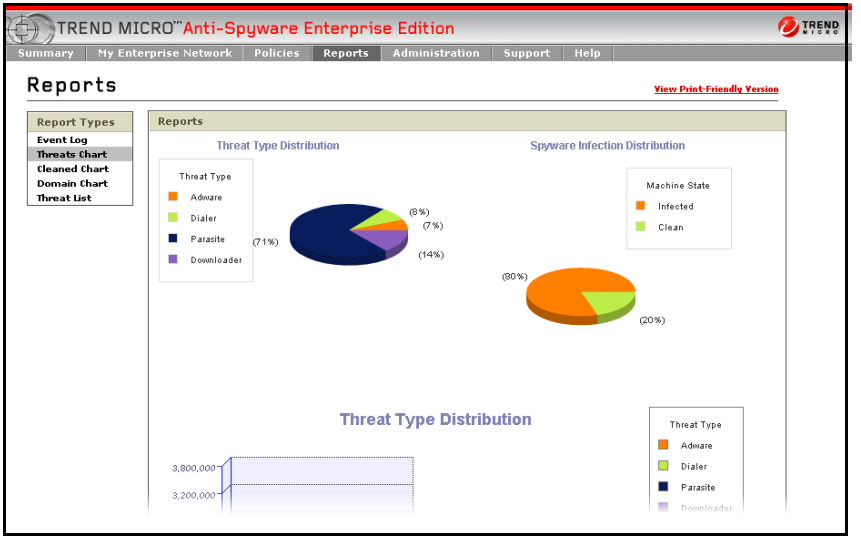


Figure 7-1: Reports screen

Report choices include:

- Threats Chart
- Cleaned Chart
- Domain Chart
- Threat List

Understanding the Threats Chart

The Threats Chart provides an overview of the threats on your network. It shows the distribution of threat types, as well as the distribution of spyware across all protected computers in your domain.

To view threat details:

1. Open the Web console.
2. Click **Reports**, then **Threats Chart**.

Understanding the Cleaned Chart

Threat Type Distribution is displayed as a pie chart and a bar graph and shows you the breakdown of the different types of threats that are currently present on your network. Spyware Infection Distribution is displayed as a pie chart and presents you with the percentage of infected and clean computers on your network. When viewing Spyware Infection Distribution on the Cleaned Threats page, it shows you percentages for computers that were at any time infected (Once Infected) and computers that have never been infected (Always Clean).

To view the cleaned chart:

1. Open the Web console.
2. Click **Reports**, then **Cleaned Chart**.

Understanding the Domain Chart

The domain chart provides an overview of the domains that have been discovered in your network environment and which of them are managed by Trend Micro™ Anti-Spyware Enterprise Edition and which are not.

To view the domain chart:

1. Open the Web console.
2. Click **Reports**, then **Domain Chart**.

Understanding the Threat List

The Threat List contains all types of spyware sorted by source (company or group), type of threat, and total threat count. This provides an overview of what threats are most prevalent in your network. From the **Threat List** screen, you can view detailed information about a threat.

To view threat chart:

1. Open the Web console.
2. Click **Reports**, then **Threat List**.
   - Click **Type** to get detailed information about the spyware type.
   - Click **Count** to get a count of the clients that found this spyware.
   - Click the spyware name to display background information on each spyware source.

   This information can be useful in isolating and identifying patterns

Chapter 8

Support

This chapter provides information on obtaining additional help from Trend Micro support. You can access general security information from the Trend Micro Web site, or search for product-specific information through the Trend Micro Knowledge Base.

Trend Micro Security Information

Comprehensive security information is available from the Trend Micro free Security Information Center. The URL for spyware information is:

`http://www.trendmicro.com/vinfo/grayware/default.asp`

Access Trend Micro Security Information to find out about:

- Security Encyclopedia—a compilation of knowledge about spyware/grayware
- Spyware/Grayware Advisories—current news about the top threats, associated risks, and pattern file update that addresses the threat
- Top 10—current list of the top ten spyware/grayware threats by number of reports

General spyware/grayware information, including:

- Safe computing guide—a description of safety guidelines to reduce the risk of spyware infections
- White papers—that explain such concepts as the real cost of a virus outbreak or how to manage email content security
- Webmaster tools—free spyware information updates and tools
- TrendLabs—the ISO 9000-certified virus research and product support center

Technical Support

A license to Trend Micro software usually includes the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one (1) year. Thereafter, you must renew Maintenance on an annual basis at Trend Micro's then-current Maintenance fees to have the right to continue receiving these services.

Contact Information

Visit our Web site at:

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

Technical Support Information

For technical support in the U.S. and Canada, contact us at:

```
support@trendmicro.com
```

For technical support outside the U.S. and Canada, contact us at:

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

Phone Numbers

- Our main U.S. phone and fax numbers are:

```
Toll free: 1-800-228-5651 (sales)
Voice: 1-408-257-1500 (main)
Fax: 1-408-257-2003
```

- To reach us outside the U.S., call:

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

- Our U.S. headquarters are located in Silicon Valley at:

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

Knowledge Base

Trend Micro provides Knowledge Base, our online knowledge database.

You can use Knowledge Base, for example, if you are having trouble receiving program file updates or if you are getting an error message. You can search Knowledge Base, using the text of the message, to find out what is causing the problem and how to fix it.

The contents of Knowledge Base are being continuously updated, and new solutions are added daily. If you are still unable to find an answer, you can email a description of the problem to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

To access the Trend Micro Knowledge Base, go to the following Web site:

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

Appendix A

Working with the Trend Micro™ Control Manager™ Agent

Trend Micro Control Manager™ is a centralized system that unites Trend Micro products and services into a cohesive security and content management solution.

This chapter discusses the following topics:

- Introducing Control Manager
- Key features
- Managing Trend Micro Anti-Spyware Enterprise Edition using Control Manager

Introducing Control Manager

Trend Micro Control Manager (TMCM) is a central management console that manages Trend Micro security products and services at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Control Manager is available in Standard and Enterprise editions to better satisfy the needs of different enterprises.

- The Standard edition provides powerful management and configuration features that allow you to manage your corporate antivirus and content security.
- The Enterprise edition is for large enterprises and xSPs. This edition adds a variety of advanced features to the Standard edition—such as cascading console support and reporting functions.

Key features

Key features of Control Manager include:

- Centralized management, which allows administrators to configure, monitor, and maintain Trend Micro software installed on the network from a single console—regardless of location or platform
- Flexible and scalable configuration, which simplifies the administration of a corporate security policy
- A hierarchical structure for job delegation so administrators can determine access control—different users can be assigned separate access to individual branches of the hierarchy

Using Trend Micro Anti-Spyware Enterprise Edition with Control Manager

Control Manager is a useful tool for organizations with multiple Trend Micro Anti-Spyware Enterprise Edition servers or for organizations using other Trend Micro products in addition to Trend Micro Anti-Spyware Enterprise Edition. The main advantages of using Control Manager with Trend Micro Anti-Spyware Enterprise Edition are:

- Centralized logging
- Reporting
- Centralized configuration
- Centralized distribution of spyware definitions

Note: For detailed information about installing the Trend Micro Control Manager server software, instructions for installing the Control Manager Agent, and information about accessing your product through the TMCM console, please refer to the Control Manager documentation.

Introducing the Control Manager Agent for Trend Micro Anti-Spyware Enterprise Edition and Trend Micro Infrastructure

A Trend Micro Anti-Spyware Enterprise Edition server has its own agent, which is responsible for the following actions:

- Receiving commands from the Control Manager server through the Communicator
- Collecting managed product status and logs, and sending them to the Control Manager server through the Communicator

The Communicator, or the Message Routing Framework, is the communication backbone of the Control Manager system. It is a component of the Trend Micro Infrastructure (TMI). Communicators handle all communication between the Control Manager server and managed products. They interact with Control Manager agents to communicate to managed products.

The Control Manager agent is an application installed on a Trend Micro Anti-Spyware Enterprise Edition server that allows Control Manager to manage the product. Agents interact with the managed product and the Communicator. An agent serves as the bridge between managed products and the Communicator. Hence, you must install the Control Manager agent for Trend Micro Anti-Spyware Enterprise Edition on the same server as the product.

After installing, Control Manager agent and TMI files can be found in the following locations on a Window-based server:

- `<root>:\Program Files\Trend\Common\TMI`
- `<root>:\Program Files\Trend Micro\Antispyware\Agent`

Installing the Trend Micro Control Manager Agent for Trend Micro Anti-Spyware Enterprise Edition

If you did not choose to install the Trend Micro Control Manager Agent for Trend Micro Anti-Spyware Enterprise Edition during the initial installation process, you can install the agent manually.

Note: You must have installed the Control Manager server software before installing the Control Manager Agent for Trend Micro Anti-Spyware Enterprise Edition.

To install the Trend Micro Control Manager Agent for Trend Micro Anti-Spyware Enterprise Edition:

1. Open the installation directory, usually `C:/Program Files/Trend Micro/Antispyware/Contol_Manager_Agent/`
2. Run the agent installation program, `Setup.exe`.
3. From the installation welcome screen, click **Next**.
4. Read the Trend Micro license agreement and click **Yes** to accept.
5. Type the name of a Control Manager account to manage Trend Micro Anti-Spyware Enterprise Edition. For more information about Control Manager Accounts, see the Trend Micro Control Manager documentation.
6. Click **Next**.
7. Configure a message routing path.
8. Click **Next**.
9. Import the public key that the Control Manager Agent will use to encrypt communication between the Control Manager server and Trend Micro Anti-Spyware Enterprise Edition.
10. Click **Next**.
11. Once installation is complete, click **OK** to close the installer.

Managing Trend Micro Anti-Spyware Enterprise Edition Using Control Manager

Once you have installed the Control Manager software on the Control Manager server and the Control Manager agent on the Trend Micro Anti-Spyware Enterprise Edition enterprise server, Control Manger will be able to communicate with Trend Micro Anti-Spyware Enterprise Edition. The Control Manager agent for Trend Micro Anti-Spyware Enterprise Edition supports the following features:

- Web console redirection
- Spyware definition file updates
- Viewing and managing spyware and event logs
- Command Tracking
- Update reporting:
  - Update successful
  - Update not successful
- Service notification if the product stops
- Reports
  - Overall List of Spyware Detected in All Entities
    - All Entities Spyware Detection Infection List
  - Overall Spyware Comparison
    - Spyware Detections
  - Overall Damage Cleanup Comparison
    - Damage Cleanup
  - Overall Most Commonly Detected Spyware
    - Top Ten Spyware Detections Points Report
  - Overall Summary of Spyware Detected
    - Total Number of Spyware Detections

For detailed information on using the Control Manager interface, see your Trend Micro Control Manager documentation.