

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 User Guide, which are available on Trend Micro's Web site at:

<http://www.trendmicro.com/download>

NOTE: A license to Trend Micro Anti-Spyware for SMB 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.

To order renewal Maintenance, you may download and complete the Trend Micro Maintenance Agreement at the following site:

<http://www.trendmicro.com/en/purchase/license/overview.htm>

Trend Micro, the Trend Micro t-ball logo, and Venus Spytrap are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Part number: ASEM32313/50620

© 2005 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Release Date: June 2005

The Getting Started Guide for Trend Micro Anti-Spyware for SMB 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>.

About Trend Micro Anti-Spyware for SMB 3

Understanding How Trend Micro Anti-Spyware Fits into Your Network	3
System Components	4
Web Console.....	4
The Server Agent	4
The Anti-Spyware Agent	5
Trend Micro Anti-Spyware Functions and Benefits	6

Installing Trend Micro Anti-Spyware 7

Pre-Installation Information	7
Connectivity and Network Rights.....	7
Configuring Your Firewall	8
System Requirements: Server	8
System Requirements: Clients	9
Installing the Trend Micro Anti-Spyware for SMB Server Software	10
Server Installation	10

Configuring Trend Micro Anti-Spyware 13

Starting Trend Micro Anti-Spyware for SMB	13
Accessing the Web Console	14
Working with the Summary Screen	15
Understanding the Summary View	16
Configuring Domains	16
Installing the Client Software	18
Deploying the Client Software Using the Console	18
Installing the Client Software Using the MSI Installer.....	23
Configuring Updates	27
Updating Spyware Definitions.....	27
Updating Trend Micro Anti-Spyware for SMB.....	27

Uninstalling the Client Software	28
Uninstalling the Client from One Desktop	28
Uninstalling the Client from Multiple Desktops.....	30

Managing Trend Micro Anti-Spyware for SMB 31

Working with the Database	31
Changing the Administrator Password	32
Licensing Trend Micro Anti-Spyware	33
Mapping Your Network	34
Viewing Domains and Desktops.....	34
Working With Remote Users.....	37
When a Desktop Is Removed from a Domain	37
When a Desktop is Moved Between Domains	37
Setting and Using Policies	38
Understanding Policy Options	38
Understanding Policy Settings.....	38
Creating a New Spyware Policy	40
Scanning and Cleaning Desktops	43
Scanning and Cleaning Automatically	43
Scanning and Cleaning Manually	43
Restoring Desktop Software	44
Working with Reports	44
Understanding the Current Threats and Cleaned Threats Reports	46
Understanding the Event Log	46
Understanding the Threat List	47

Support 49

Trend Micro™ Security Information	49
Technical support	50
Contact information	50
Knowledge Base	51

About Trend Micro Anti-Spyware for SMB

Trend Micro Anti-Spyware for SMB (Small and Medium Businesses) 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 Fits into Your Network

Trend Micro Anti-Spyware for SMB is based on a client/server model. The administrative 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 administrative server and clients.

System Components

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

Web Console

The console provides a Web-based interface for administrators to manage the administrative server and deploy and manage spyware protection throughout the network.

From the console, you can easily deploy a scalable population of desktops. The Web-based console provides convenience and flexibility. While most console work is from a server, the console provides the option of managing the process from just about any desktop in the organization. This also allows access to network desktops through the variety of firewall configurations that might be deployed in your organization.

The administrative 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 administrative server where Trend Micro Anti-Spyware for SMB 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 administrative 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 administrative server to receive configuration and spyware definition database updates. The client also transmits client activity reports back to the administrative 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 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 administrative 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.

Venus SpyTrap™

The Anti-Spyware Agent includes Venus Spy Trap™, a unique technology for active, predictive monitoring, which serves as an early warning system. The technology proactively stops spyware by checking programs against known spyware signatures before they are actually run on a desktop. This is an important feature as it prevents damage and potential theft of data from occurring on the user's system. This exclusive capability operates in the background and provides real-time network desktop protection.

CWShredder™

Trend Micro Anti-Spyware for SMB 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 for SMB.

Trend Micro Anti-Spyware Functions and Benefits

Trend Micro Anti-Spyware for SMB 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 scanning 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 38.

Installing Trend Micro Anti-Spyware

This chapter outlines a step-by-step process for deploying Trend Micro Anti-Spyware for SMB on the server. It provides pre-installation information, system requirements, and a walk-through of the product installation. 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 18.

Pre-Installation Information

To prepare for the installation of Trend Micro Anti-Spyware for SMB, you will need to configure your firewall and verify that the administrative server, client desktops, and the network meet the configuration requirements outlined below.

Connectivity and Network Rights

For the administrative server to administer a desktop it must have TCP connectivity to the desktop. To automatically install a desktop, the administrative 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 23.

Note: A different Trend Micro Anti-Spyware for SMB 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:

- tmassa.exe
- tmasca.exe
- reminst.exe
- imclntinst.exe

System Requirements: Server

Identify the Windows-based platform that is going to host the administrative server. This platform must not have an existing instance of MySQL. The server hosting the product must have a static IP address; it cannot obtain its IP address using DHCP.

The Trend Micro Anti-Spyware for SMB software can be installed on a workstation or server located in the network management or IT workspace and should meet the following configuration requirements:

- Windows XP Professional, 2000, 2000 Server, 2003 Server
- 256MB RAM
- 5GB disk space
- Internet Explorer 5.5 and above, required to access the Web-based user interface of the administrative server

System Requirements: Clients

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

- Windows XP Professional, 2000, 2000 Server, 2003 Server

Note: Trend Micro Anti-Spyware for SMB client software can be installed on platforms running Windows 2000, 2000 Server, XP Professional, and Server 2003.

- 128MB RAM
- 5MB disk space

Note: For client computers running Windows XP Service Pack 2, 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 8080), NetBIOS ports (137, 138, 139, 445), and socket mode using port (default 54447) to your firewall exceptions. Consult your Windows help file for more information.

Installing the Trend Micro Anti-Spyware for SMB Server Software

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

Server Installation

On server that is going to host the administrative server, download the Trend Micro Anti-Spyware installation program from the Trend Micro Web site, or open it from the Trend Micro Enterprise CD.

The installation program prompts you through the following steps:

1. Register Trend Micro Anti-Spyware for SMB. There are two choices:
 - Enter your Activation Code
 - Register on-line to receive a code via email.

Note: Skip this step to register later.

2. Agree to the Trend Micro Anti-Spyware license.
3. Enter the administrator's email address for communications about spyware definition database updates and product updates from Trend Micro.
4. Select an installation path.
5. Set up the Domain Administrative account. Enter a username 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.
6. Select a user name and password for administrator access to the Web console.

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

7. Select the port that Trend Micro Anti-Spyware for SMB will use for communication between the server and clients.

Note: This port must not be in use by Windows IIS or any other Web server products.

8. The installation will load components, including:
 - An Apache Web server
 - 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. Access the administrative server Web console by clicking this link, to configure the policies and other settings of Trend Micro Anti-Spyware for SMB. You can also access the Web console remotely, by typing the IP address or host name and port number of the administrative server in your Web browser.

For more information, see *Configuring Trend Micro Anti-Spyware* starting on page 13.

Configuring Trend Micro Anti-Spyware

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

Once the software is configured, see *Configuring Updates* starting on page 27 for information on keeping your spyware definitions up to date, and *Managing Trend Micro Anti-Spyware for SMB* starting on page 31 for detailed information on using the product.

Starting Trend Micro Anti-Spyware for SMB

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 from any computer in your network that is connected to the server via HTTP.

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 to access the login screen.

Initially, the **Summary** screen shows all desktops as “Not Installed” until the Client Agent deployment process has started. A desktop shown as “Not Installed” does not have the Trend Micro Anti-Spyware Client Agent installed on it. An “Installed” desktop is one that has the Trend Micro Anti-Spyware Client Agent installed and protecting it from threats.

Using the Navigation Bar

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



Figure 3-1: 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
- Clicking **User Guide** 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.

TREND MICRO Anti-Spyware for Small and Medium Businesses 3.0

Summary | My Network | Policies | Reports | User Guide | Support

Summary

Summary	
License Status:	Full-Activated
Seats Number:	25
Licenses In Use:	8
Expiration Date:	Mon Jun 27, 2005
Days Until Expiration:	4
Console IP Address:	10.2.160.15
Console Version:	3. 0. 0. 18
Build Version:	3. 0. 0. 18
Definition Version:	2.75
Discovered Domains:	15
Total Desktops	695
Installed Desktops:	12
Not Installed Desktops:	683
Total Threats:	24
Total Cleaned:	54

Administration	
Database Admin	Change Password
View License	Renewal Instructions

NOTE: Passwords can only be changed while accessing the console from a local browser.

Figure 3-2: 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.

Configuring Domains

The first step in configuring Trend Micro Anti-Spyware for SMB is 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.

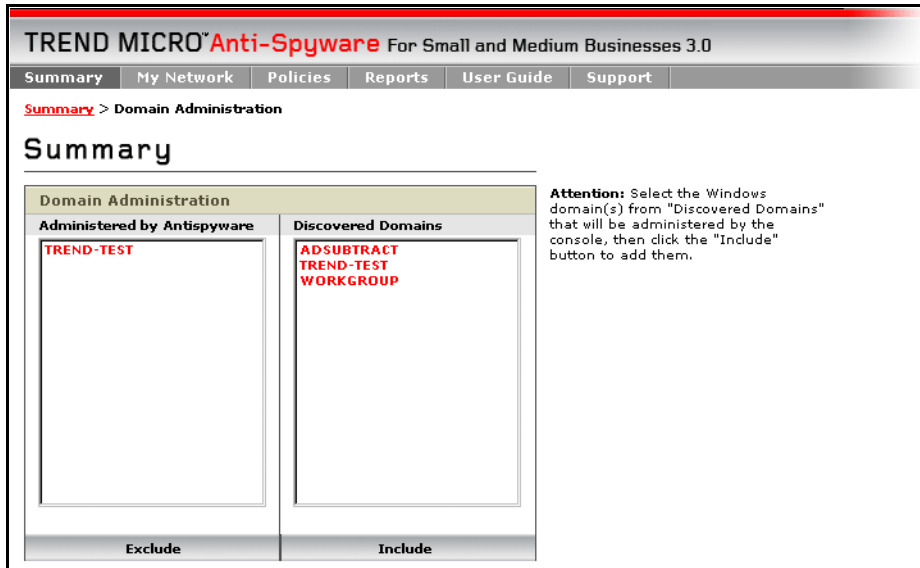


Figure 3-3: Domain administration screen

To configure the domains that this server will administer:

1. Open the Web console.
2. From the **Summary** screen, click the **Discovered Domains** count.
3. On the **Domain Administration** screen, select the domains to be administered by the console.
4. Click **Include**. This starts the periodic desktop discovery process by the console.

To exclude domains from the periodic desktop discovery process:

1. Open the Web console.
2. From the **Summary** screen, click the **Discovered Domains** count.
3. On the **Domain Administration** screen, select the domains to exclude from discovery.
4. Click **Exclude**.

Trend Micro Anti-Spyware for SMB will not attempt automatic discovery of new machines in domains in the Exclude list.

Installing the Client Software

There are two choices for installing the Trend Micro Anti-Spyware for SMB 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 23.

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.

The screenshot shows the 'My Network' screen in the Trend Micro Anti-Spyware console. The interface includes a navigation menu with 'Summary', 'My Network', 'Policies', 'Reports', 'User Guide', and 'Support'. The main content area is titled 'My Network' and features a 'View Print-Friendly Version' link. Below this is a table with columns for 'Names', 'User', 'Domains', 'Threats', 'Cleaned', 'Policies', 'Status', 'Agent', and 'Definitions'. The table is filtered by 'TREND-TEST:1' and 'Global_Default'. It lists 13 desktop nodes, each with a name starting with 'Node_' followed by a number and a date. All nodes show 50 threats and 0 cleaned items, and are all in an 'Installed' status.

Names	User	Domains	Threats	Cleaned	Policies	Status	Agent	Definitions
1 Node_ 0		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
2 Node_ 10		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
3 Node_ 100		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
4 Node_ 1000		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
5 Node_ 10000		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
6 Node_ 10005		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
7 Node_ 10010		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
8 Node_ 10015		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
9 Node_ 10020		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
10 Node_ 10025		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
11 Node_ 10030		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
12 Node_ 10035		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67
13 Node_ 10040		TREND-TEST:1	50	0	Global_Default	Installed	1. 0. 1. 87	2.67

Figure 3-4: My Network screen—desktop discovery

Deploying the Client Using Automatic Installation

You can configure Trend Micro Anti-Spyware for SMB to install the Client Agent on all clients 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 Network** screen, confirm that all desktops have been discovered by the administrative server.

2. Add a new policy by clicking **Policies** to open the **Policies** screen.

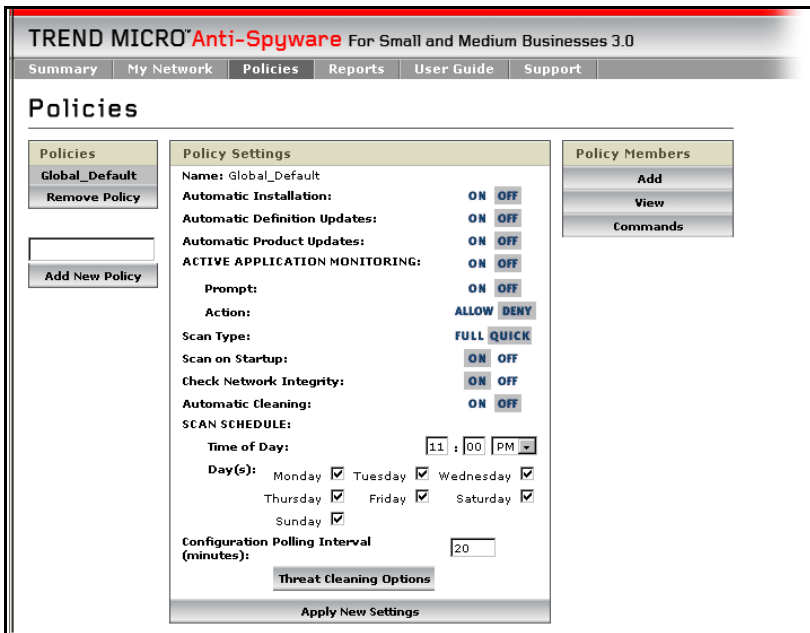


Figure 3-5: The Policies screen

3. Type a name for your new policy in the field on the left, then click **Add New Policy**.

Note: Choose a descriptive name for the policy that will help you distinguish this policy from others when managing policies in the future.

4. Select the desktops that this policy will apply to by clicking **Add** under **Policy Members**:
 - a. Under **Domains** in the **Policy Non-members** list, click the domain that contains the desktops to add.
 - b. Select desktops from the **Desktops** list.
 - c. Click **Add Members** to add the selected desktops to the current policy.

5. Select **Automatic Installation** if it has not been selected for the new policy.
6. Click **Apply New Settings**, and installation will begin immediately for that policy group.
7. Return to the **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.

Deploying the Client Using Manual Installation

You can manually install the Trend Micro Anti-Spyware for SMB 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 Network** on the navigation bar.
2. Find the desktop in question by using the **My Network** sort tool, sorting by domain or by policy.
3. Click on the name of the desktop where the agent will be installed. The **Desktop Status** box opens.

- Click **Install** in the Desktop Status box. The status for this desktop will change to “Installed.”

TREND MICRO[™] Anti-Spyware For Small and Medium Businesses 3.0

Summary | My Network | Policies | Reports | User Guide | Support

My Network > Desktop

My Network

Domains	Desktops	Desktop Status
TREND-TEST: 1	Desktops: 135 US-DANIELH 136 US-DANIELY 137 US-DANIELYANG 138 US-DANJACKOBS 139 US-DARRENBUI 140 US-DAVIDLIE 141 US-DAVIDST42 142 US-DEBV-T23 143 US-DEVNAV 144 US-DONCAMP 145 US-DVPDB 146 US-ELIZALINT42 147 US-EPCOTMNL 148 US-FRANKKT30 149 US-	Name: US-DANIELH User: Status: Not Installed Remote Status: Not Running License Status: Scan Only Comm Mode: Domain Last Scan: NA Last Contact: May 27, 2005, 1:08 pm Policy: Global_Default Domain: TRENDUS IP Address: NA Client Version : NA Build Version : NA Definition Version : NA Current Threats : 0 Total Cleaned: 0 Install

Figure 3-6: My Network screen—installation

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.

Note: 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 such as firewalls that might prevent proper operation. 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 for SMB 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 18.

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 5449
- 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, 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 for SMB can be deployed utilizing the client MSI (Microsoft Installer) installation tool.

Understanding the Trend Micro Anti-Spyware for SMB MSI Command Line Parameters

The following command line is used for manual deployment:

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

Understanding the Command Line Parameters

The following section describes command line parameters and their values.

```
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 Type>

This is an optional parameter that specifies how the client expects the server to communicate with it. One of three values can be specified:

- 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 the default, you must configure all clients and the server must use the same port. Call the Server Agent using the /port switch to configure a port other than the default.

For example C:/tmassa.exe /port 8088

- 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.
- 3—indicates the client will be set in 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=1 CMDINT=xxx
```

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

/Lve <log file name>

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

/qn

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

Command Line Examples

For a new installation, use the following command structure:

```
msiexec /i tmasclnt.msi ALLUSERS=1
REBOOTREALLYSUPPRESS=No /Lve tmasclnt.log /qn
SERVERIP=xxx.xxx.xxx.xx SERVERPORT=x CMDMODE=x CMDINT=x
SOCKET=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 REBOOTREALLYSUPPRESS=No /Lve tmasclnt.log /qn
SERVERIP=xxx.xxx.xxx.xx SERVERPORT=x CMDMODE=x CMDINT=x
SOCKET=x
```

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

Configuring Updates

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

Updating Spyware Definitions

Trend Micro periodically issues spyware definition updates as new threats are identified. The Trend Micro Anti-Spyware for SMB server automatically downloads definition updates from the Trend Micro ActiveUpdate server. This helps to keep the spyware definitions current.

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.

Note: Trend Micro recommends configuring all policies to use **Automatic Definition Update** to ensure up-to-date protection for desktops in your network.

Updating Trend Micro Anti-Spyware for SMB

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

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: If Trend Micro Anti-Spyware for SMB is configured to use domain mode and you have installed the desktops from the console, the client software cannot be uninstalled locally.

Uninstalling the Client from One Desktop

To uninstall the client software from a desktop:

1. Open the Web console.
2. Click **My Network** in the navigation bar.
3. Select the appropriate domain.

4. Locate and select the desktop to be uninstalled.

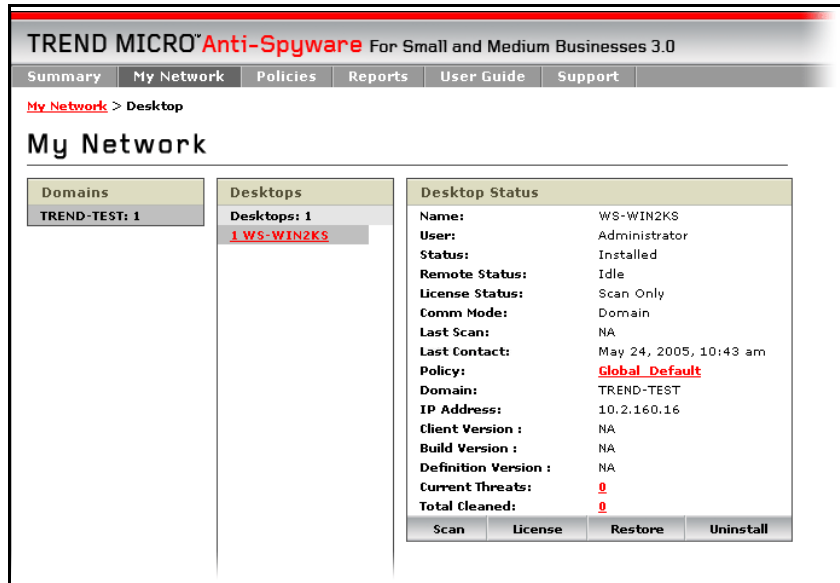


Figure 3-7: My Network screen—uninstallation

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

Note: If the client is deleted, but the desktop is still part of your network, when the Trend Micro Anti-Spyware for SMB client is removed, the desktop will still be recognized in the periodic discovery process. It will be listed on the **Summary** screen and **My 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 **Policies** in the navigation bar.
3. Select the policy that contains the desktops.
4. Click **Policy Members**.
5. Click **Commands** to open the **Policy Members Commands** screen.

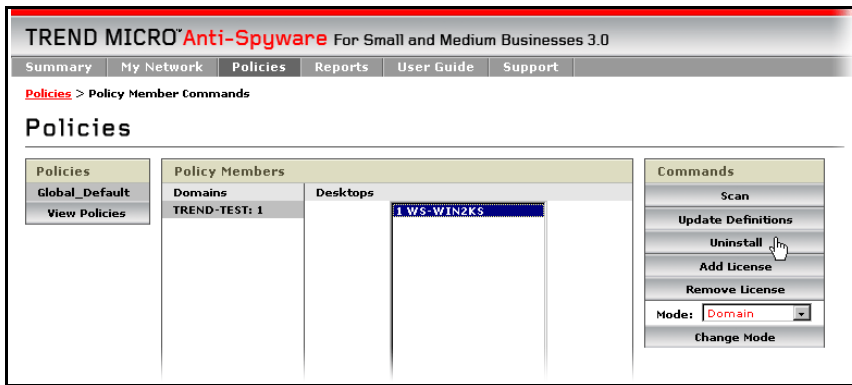


Figure 3-8: Policies screen—commands

6. Select the desktops to uninstall.
7. 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, when the Trend Micro Anti-Spyware for SMB client is removed, the desktop will still be recognized in the periodic discovery process. It will be listed on the **Summary** screen and **My Network** screen and its status will be “Uninstalled.”

Managing Trend Micro Anti-Spyware for SMB

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

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, add or remove the client software from a desktop, or administer the **Event Logs** and **Activity History**.

The screenshot shows the 'Database Administration' screen in the Trend Micro Anti-Spyware web console. The interface is organized into several panels:

- Reset Counts:** Includes checkboxes for 'Total Threats' and 'Total Cleaned', and an 'Apply New Settings' button.
- Domains & Desktops:**
 - REMOVE DOMAIN:** A form with a 'Domain:' field and an 'Apply New Settings' button.
 - REMOVE DESKTOP:** A form with 'Domain:' and 'Desktop:' fields, an 'Advanced' checkbox, and an 'Apply New Settings' button.
 - ADD DESKTOP:** A form with 'Domain:', 'Desktop:', and 'IP Address:' fields, and an 'Apply New Settings' button.
- Event Log:**
 - PURGE EVENT LOG:** A form with 'Purge Date (YYYY-MM-DD):' field and an 'Apply New Settings' button.
 - EVENT LOG HISTORY:** A form with a 'Number of Days' input field (set to 30) and an 'Apply New Settings' button.
- Activity History:**
 - PURGE ACTIVITY HISTORY:** A form with 'Purge Date (YYYY-MM-DD):' field and an 'Apply New Settings' button.
 - ACTIVITY HISTORY:** A form with a 'Number of Days' input field (set to 30) and an 'Apply New Settings' button.
 - Set Entries Per Page:** A form with an 'Entries' input field (set to 500) and an 'Apply New Settings' button.

The top navigation bar includes links for 'Summary', 'My Network', 'Policies', 'Reports', 'User Guide', and 'Support'. The breadcrumb trail shows 'Summary > Database Administration'.

Figure 4-1: Summary screen—database administration

To manage the database:

1. From the **Summary** screen, click **Database Admin**.
The Database Administration screen opens, as shown in the previous figure.
2. Make any configuration changes:
 - **Reset Counts**—resets the threat and cleaning counters to zero
 - **Domains & Desktops**—
 - **Remove Domain**—removes a domain from the list of recognized domains
 - **Remove Desktop**—removes the client software from a desktop
 - **Add Desktop**—allows you to manually install the client software on a desktop
 - **Event Log**—
 - **Purge Event Log**—deletes all items from the event logs
 - **Event Log History**—allows you to configure the number of days events should be kept in the log
 - **Activity History**—
 - **Purge Activity History**—deletes all items from the activity history
 - **Activity History**—allows you to configure the number of days the history should be kept
 - **Set Entries Per Page**—allows you to configure the number of entries shown on each page
3. Click **Apply New Settings** to apply the changes.

Changing the Administrator Password

From the **Summary** screen, you can change the domain or console's username and password.

To change the password:

1. Open the Web console.

TREND MICRO Anti-Spyware for Small and Medium Businesses 3.0

Summary My Network Policies Reports User Guide Support

Summary

Summary	
License Status:	Full-Activated
Seats Number:	25
Licenses In Use:	8
Expiration Date:	Mon Jun 27, 2005
Days Until Expiration:	4
Console IP Address:	10.2.160.15
Console Version:	3. 0. 0. 18
Build Version:	3. 0. 0. 18
Definition Version:	2.75
Discovered Domains:	15
Total Desktops	695
Installed Desktops:	12
Not Installed Desktops:	683
Total Threats:	24
Total Cleaned:	54

Administration	
Database Admin	Change Password
View License	Renewal Instructions

NOTE: Passwords can only be changed while accessing the console from a local browser.

Figure 4-2: Summary screen

2. From the **Summary** screen, click **Change Password**.
3. Type the old password.
4. Type and confirm the new password.
5. Click **Apply New Password**.

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

Licensing Trend Micro Anti-Spyware

You can view the status of your product license and enter a new Activation Code from the **Summary** screen.

To enter a new Activation Code:

1. Open the Web console.
2. From the **Summary** screen, click **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**.

Mapping Your Network

Trend Micro Anti-Spyware for SMB maps your network to determine which domains are available and discover the computers that belong to each domain. This step is essential to creating policies and applying them consistently across your network environment.

Viewing Domains and Desktops

To ensure that Trend Micro Anti-Spyware is configured to recognize all the domains and desktops on your network, use the **My Network** view.

To view your network:

1. Open the Web console.
2. Select **My Network** on the navigation bar to move to the **My Network** screen.
3. **To view computers in a specific domain:**
 - a. Select a domain.
 - b. Click **Refresh**.

This screen shows the status of all desktops and domains identified in the discovery process. For each desktop, the first-level screen shows threats, cleaned, policy name, client agent installation status, agent version and spyware definitions version.

Upon initial installation, inspect the listings to be sure that all expected desktops are listed. Unconnected desktops or desktops with faulty communications do not appear on the **My Network** screen.

A sort tool at the top of the desktop list allows you to sort several selected parameters. Select a domain and click **Refresh**. This will show the desktops in the domain selected. Inspect the listings for each domain.

The desktop population can be sorted by additional parameters including Policy. This is used to track status and changes for a given policy.

Managing Desktops

Clicking on any desktop will show a **Desktop Status** box with detailed client desktop discovery data, including desktop Name, Remote (client agent) Status, Domain, Remote Status (such as scanning, cleaning or idle), IP Address, software and definition versions, threats, cleans and other information. The screen also identifies the domain and other desktops in that domain.

The screenshot shows the Trend Micro Anti-Spyware interface for Small and Medium Businesses 3.0. The main navigation bar includes Summary, My Network, Policies, Reports, User Guide, and Support. The current view is 'My Network > Desktop'. The 'My Network' section is divided into three panes: Domains (showing TREND-TEST: 1), Desktops (showing 1 WS-WIN2KS), and Desktop Status (showing details for WS-WIN2KS). The Desktop Status pane includes fields for Name, User, Status, Remote Status, License Status, Comm Mode, Last Scan, Last Contact, Policy, Domain, IP Address, Client Version, Build Version, Definition Version, Current Threats, and Total Cleaned. At the bottom of the Desktop Status pane are buttons for Scanning and Reset.

TREND MICRO™ Anti-Spyware For Small and Medium Businesses 3.0	
Summary	My Network
Policies	Reports
User Guide	Support
My Network > Desktop	
My Network	
Domains	Desktops
TREND-TEST: 1	Desktops: 1
	1 WS-WIN2KS
	Desktop Status
Name:	WS-WIN2KS
User:	Administrator
Status:	Quick Scan Started
Remote Status:	Not Running
License Status:	Scan Only
Comm Mode:	Domain
Last Scan:	NA
Last Contact:	May 20, 2005, 2:38 pm
Policy:	Global Default
Domain:	TREND-TEST
IP Address:	10.2.160.16
Client Version :	NA
Build Version :	NA
Definition Version :	NA
Current Threats:	0
Total Cleaned:	0
Scanning. Reset	

Figure 4-3: My Network screen—desktops

Options for Scan, Clean, Restore and Uninstall are also provided in the controls at the bottom of the **Desktop Status** box. For desktops that do not have a full license, the **Clean** button is replaced with a **License** button which is used to add a full license to the desktop. These are discussed in *Scanning and Cleaning Desktops* starting on page 43.

Changes in the Client Network

If a new desktop is added to a domain, the periodic Trend Micro Anti-Spyware for SMB discovery process will identify the new client in the **Summary** screen and the

My Network screen. The new desktop is automatically assigned to the Global Default policy. If Automatic Installation for the Global_Default policy has been turned on, the client software is installed on the desktop. Spyware protection starts immediately, using the settings configured in the Global_Default policy. The desktop can 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 for SMB 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 can 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 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 may want to remove the old entry to avoid confusion.

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 Policy Options

By default all desktops in the network are initially assigned to the Global_Default policy. You can modify the Global_Default settings, adding one or more new policies, deleting policies, and moving groups of desktops to 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."
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 threats attempting to start execution on the desktop. You can deny all spyware processes, allow all spyware processes, or present the user with a dialog and let him/her make the decision.

Setting	Explanation
Scan Type	<ul style="list-style-type: none">• 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 for SMB automatically starts a scan at the specified day and time.
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.

Creating a New Spyware Policy

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. Type the name of the new policy into the field on the left.
4. Click **Add New Policy**.
5. Configure the settings for the new policy.
6. Click **Apply New Settings** to apply your changes to the policy.

Applying Policies to Policy Groups

The **Policy Members** box on 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 38.

To apply policies to groups:

1. Open the Web console.
2. Click **Policies** in the navigation bar.
3. Select a policy.
4. Click **Commands**.

This opens the **Policy Members Commands** screen.

5. From here, you can:
 - **Scan** of a desktop or group of desktops.
 - **Update Definitions** on a desktop or group of desktops.
 - **Uninstall** the client software from a desktop or group of desktops.

Note: Select multiple desktops using the Ctrl or Shift key.

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 **Policy** screen using the navigation bar.
3. Select the existing policy from the left column.
4. Change the policy settings in the center column.
5. Click **Apply New Settings** 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.

Creating an Exclude List

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

To create an Exclude List:

1. Open the Web console.
2. Click **Policies** on the navigation bar.
3. In the **Policy Settings** box, select the **Threat Cleaning Options** button.
This opens a **Threats** dialog showing the policy's **Included Threats** and **Excluded Threats**.

Note: When you initially create a policy, all security risks are **Included**.

4. 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 items by holding down the **CTRL** key.

5. After you have finished selecting sources to exclude, click **Apply New Settings**.

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 for SMB 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 44 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 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.
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.

Restoring Desktop Software

There may be time when you need to restore a cleaned application to a desktop.

To restore recent occurrences of cleaned threats on a desktop:

1. Open the Web console.
2. Click **My Network** on the navigation bar.
3. Under **Desktop Names**, select the desktop in question.
This will open the **Desktop Status** box.
4. Click **Restore**.
The **Restore** screen opens, showing recent cleanings for that desktop.
5. Select a clean point and click **Restore**.
The items included in the selected clean points will be restored.

Working with Reports

Trend Micro Anti-Spyware for SMB 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. These extensive reporting capabilities derive from the powerful MySQL database architecture. This design permits numerous query possibilities, resulting in a choice of reports that keep the network administrator fully informed about all 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>.

To view reports:

1. From the Web console, click **Reports**.

2. Choose the type of report to view

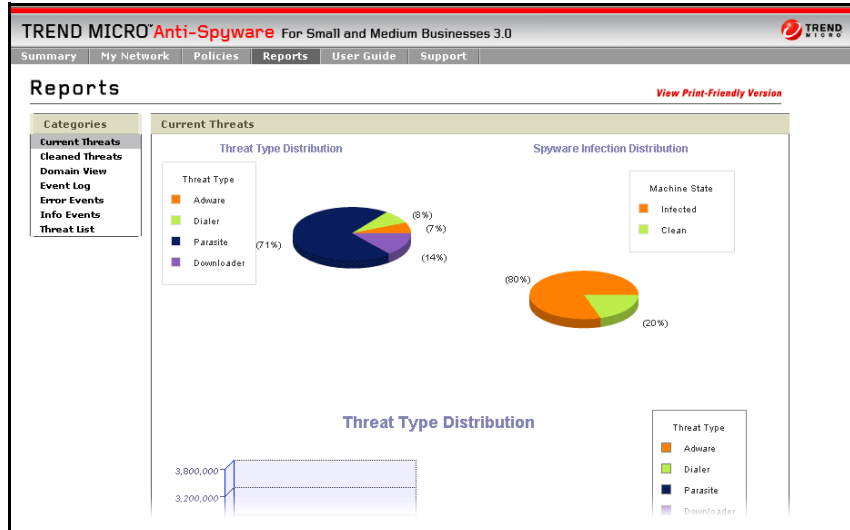


Figure 4-4: Reports screen

Report choices include:

- Current Threats
- Cleaned Threats
- Domain View
- Events Reports

Understanding the Current Threats and Cleaned Threats Reports

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).

Understanding the Event Log

The Event Log maintains a record of all desktop activities related to Trend Micro Anti-Spyware for SMB. 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, or desktop.

Understanding the Threat List

The Threat List contains all the 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, you can view detailed information about a threat.

To view threat details:

1. Open the Web console.
2. Click **Reports**, then **Threat List**.
3. Clicking on a line will provide background information on each spyware source. This information can be useful in isolating and identifying patterns.

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 Virus Information Center. The URL is:

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

Access Trend Micro™ Security Information to find out about:

- Virus advisories—current news about the top threats, associated risks, and pattern file update that addresses the threat
- Weekly Virus Report—current news about threats that have appeared in the past week
- Virus map—a description of threats by location worldwide
- Virus Encyclopedia—a compilation of knowledge about all known viruses
- Test files—a test file for testing InterScan VirusWall, and instructions for performing the test

General virus information, including:

- Virus Primer—an introduction to virus terminology and a description of the virus life cycle
- Safe computing guide—a description of safety guidelines to reduce the risk of virus infections
- Risk ratings—a description of how viruses are classified as Very Low, Low, Medium, or High threats to the global IP community
- White papers—that explain such concepts as the real cost of a virus outbreak or how to manage email content security
- Webmaster tools—free virus 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

In the U.S., Trend Micro representatives can be reached by phone, fax, or email.

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:

solutionbank.trendmicro.com/solutions/solutionSearch.asp

