



Threat Mitigator²

Administrator's Guide



Endpoint Security



Network Security

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

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

Trend Micro, the Trend Micro logo, OfficeScan, and Network VirusWall are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2008-2009 Trend Micro Incorporated. All rights reserved.

Document Part No. APEM23650/80522

Release Date: October 2009

Patents Pending

The user documentation for Trend Micro™ Threat Mitigator 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.

Detailed information about how to use specific features within the software is available in the online help file and online Knowledge Base at the Trend Micro Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Contents

Preface

Documentation	viii
Audience	ix
Document Conventions	ix

Chapter 1: Introducing Threat Mitigator

New In This Release	1-2
About Threat Mitigator	1-4
Threat Mitigation	1-4
On-demand Scan	1-6
Threat Mitigator Integration	1-6
Key Features and Benefits	1-8

Chapter 2: Installing or Upgrading Threat Mitigator

Threat Mitigator System Requirements	2-2
Pre-installation Guidelines	2-3
Threat Mitigator Placement	2-3
Threat Mitigator Capacity	2-3
Network VirusWall Enforcer Installations	2-5
Integration with Other Trend Micro Products	2-6

Threat Mitigator Fresh Installation	2-7
Setting Up the VMware Server	2-7
Setting Up the VMware Client	2-8
Setting Up Threat Mitigator	2-10
Phase 1: Preparing the Threat Mitigator Installation Package	2-10
Phase 2: Installing Threat Mitigator	2-11
Phase 3: Configuring the IP Address	2-27
Threat Mitigator and Threat Management Agent Upgrades	2-31
Threat Mitigator Uninstallation	2-33

Chapter 3: Getting Started

The Product Console	3-2
Product Console Password	3-6
Product License and Activation Code	3-7
System Time	3-7
Threat Management Services Registration	3-8
Component Updates	3-10
Threat Mitigator Components	3-10
Update Process	3-12
Update Source	3-13
Update Methods	3-14
Manual Updates	3-14
Scheduled Updates	3-15
Proxy Settings	3-16
Smart Scan Server Setup	3-17
Smart Scan Server Installation	3-17
Smart Scan Server Settings	3-18

Chapter 4: Deploying Threat Management Agents

Agent System Requirements	4-2
Agent Deployment Methods	4-3
Agent Deployment Using the Packager Tool	4-4
Package Deployment Using Active Directory	4-6
Package Deployment Using Microsoft SMS	4-7
Package Deployment Using Logon Script	4-9
Package Deployment Using a Shared Folder	4-9
Agent Deployment Using Browser-based Installation	4-10
Agent Deployment Using TMAgent Manager	4-12
TMAgent Manager Benefits	4-12
TMAgent Manager Installation	4-13
Agent Deployment	4-16
Post-installation	4-20
Recommended Tasks	4-20
Agent Settings	4-21
Agent Uninstallation	4-22

Chapter 5: Performing Threat Mitigation

Mitigation Settings	5-2
Data Sources	5-2
Mitigation Exceptions	5-5
Email Notifications	5-6
Mitigation Tasks	5-7
Threat Management	5-10

Chapter 6: Performing On-demand Scan

On-demand Scan Requirements	6-2
Smart Scan Server	6-2
Endpoint System Requirements	6-3
On-demand Scan Settings	6-5
Threat Mitigator Components	6-7
Running On-demand Scan	6-7
On-demand Scan on Agentless Endpoints	6-7
On-demand Scan on Endpoints with Agents	6-12

Chapter 7: Managing Logs

Threat Event Logs	7-2
Mitigation Status	7-4
System Logs	7-13
Log Transmission to a Syslog Server	7-14
Log Maintenance	7-15

Chapter 8: Performing Administrative Tasks

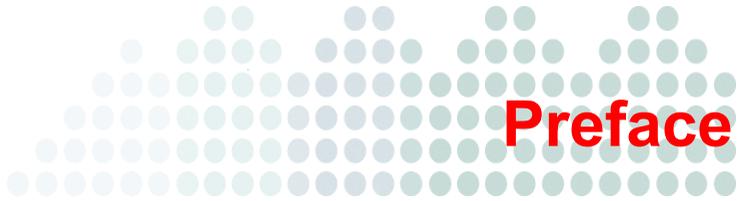
HTTPS Certificate	8-2
Administrative Accounts	8-3
Access Control	8-4
SNMP Settings	8-5
IP Address Settings	8-8
Static Route Settings	8-9
Configuration Backup and Restore	8-10
Threat Mitigator Restart	8-11
Support Tools	8-12
Appliance Firmware Flash Utility	8-13

Chapter 9: Troubleshooting and Support

Debug Information	9-2
Endpoint Debug Information	9-2
Threat Mitigator Debug Information	9-3
Troubleshooting	9-4
Device Settings and Configuration	9-4
Endpoint Settings	9-4
Contacting Trend Micro	9-7
Technical Support	9-7
The Trend Micro Knowledge Base	9-8
Security Information Center	9-9
TrendLabs	9-9
Sending Suspicious Files to Trend Micro	9-10
Documentation Feedback	9-10

Appendix A: Glossary

Index



Preface

Welcome to the Trend Micro™ Threat Mitigator Administrator's Guide. This manual contains information on installing and configuring Threat Mitigator.

This preface discusses the following topics:

- *Documentation* on page viii
- *Audience* on page ix
- *Document Conventions* on page ix

Documentation

The Threat Mitigator documentation consists of the following:

TABLE P-1. Threat Mitigator documentation

DOCUMENTATION	DESCRIPTION
Help	HTML files compiled in WebHelp format that provide "how to's", usage advice, and field-specific information. The Help is accessible from the product console when you click the Help icon  .
Administrator's Guide	A PDF document that discusses Threat Mitigator and Threat Management Agent installation, getting started information, and product configurations
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation
License Agreement	License agreements for Threat Mitigator and third-party applications
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site: http://esupport.trendmicro.com/support

The Administrator's Guide, Readme file, and License Agreement are available in the Threat Mitigator Solutions CD and at:

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

Audience

The Threat Mitigator documentation is written for IT managers and network administrators in medium and large enterprises. The documentation assumes a basic knowledge of security systems, including:

- Antivirus and content security protection
- Network concepts (such as IP address, Subnet Mask, LAN settings)
- Network devices and their administration
- Network configuration (such as the use of VLAN, SNMP)

Document Conventions

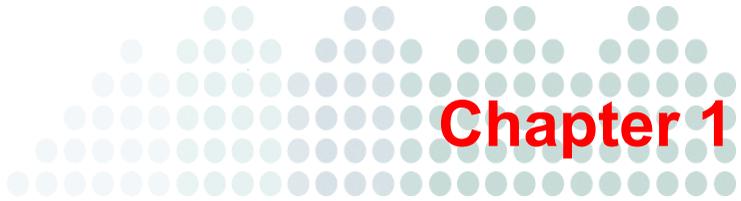
To help you locate and interpret information easily, the Threat Mitigator documentation uses the following conventions.

TABLE P-2. Document conventions

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
<i>Italics</i>	References to other documentation or new technology components
PATH: TOOLS > CLIENT TOOLS	A "breadcrumb" found at the start of procedures that helps users navigate to the relevant product console screen. Multiple breadcrumbs means that there are several ways to get to the same screen.
<Text>	Indicates that the text inside the angle brackets should be replaced by actual data. For example, C:\Program Files\ <code><file_name></code> can be C:\Program Files\sample.jpg.

TABLE P-2. Document conventions (Continued)

CONVENTION	DESCRIPTION
<hr/> Note: text <hr/>	Provides configuration notes or recommendations
<hr/> Tip: text <hr/>	Provides best practice information and Trend Micro recommendations
<hr/> WARNING! text <hr/>	Provides warnings about activities that may harm computers on your network



Introducing Threat Mitigator

This chapter introduces Threat Mitigator features and capabilities.

This chapter includes the following topics:

- *New In This Release* on page 1-2
- *About Threat Mitigator* on page 1-4
- *Threat Mitigator Integration* on page 1-6
- *Key Features and Benefits* on page 1-8

New In This Release

This Threat Mitigator version includes the following new features and product enhancements:

TABLE 1-1. New features and product enhancements

NEW FEATURES	DESCRIPTION
On-demand Scan	<p>On-demand Scan offers the same type of protection provided by endpoint security software (such as Trend Micro Internet Security™) but does not require software to be installed on the endpoint.</p> <p>On-demand Scan is intended primarily for agentless endpoints, where routine threat mitigation tasks cannot be performed. It can also be run on endpoints with Threat Management Agent to complement routine threat mitigation tasks performed by the agent.</p> <p>For details about On-demand Scan, see Performing On-demand Scan on page 6-1.</p>
Smart scan	<p>Threat Mitigator leverages Trend Micro smart scan technology during routine mitigation tasks and On-demand Scan.</p> <p>For details about Smart Scan, see Smart Scan Server Setup on page 3-17.</p>
Threat management	<p>A new Threat Management page allows you to:</p> <ul style="list-style-type: none"> • Identify endpoints that require mitigation, or endpoints that encountered On-demand Scan problems. • Run tasks on specific endpoints, such as cleanup, On-demand Scan, or custom pattern deployment. • Submit a case to TrendLabs through Threat Management Services so that a dedicated Trend Micro security expert can analyze the case (based on the data collected from the endpoint) and issue a custom pattern, if necessary. <p>For details, see Threat Management on page 5-10.</p>

TABLE 1-1. New features and product enhancements

NEW FEATURES	DESCRIPTION
Scan type	<p>After deploying a custom pattern, you can now choose to run a quick or full scan on the endpoint.</p> <p>For details, see step 3 in Mitigation Tasks on page 5-7.</p>
Agent installation	<p>Allow users to install Threat Management Agent by providing them a URL that launches the agent installation program. You can also use the Packager tool to create an agent installation package that can be deployed to many endpoints.</p> <p>For details, see Agent Deployment Methods on page 4-3.</p>
Mitigation action	<p>Enhanced threat mitigation on endpoints allows administrators to configure threat mitigation tasks, submit cases to TrendLabs, and deploy custom patterns to specific endpoints.</p>
Data sources	<p>A wider range of data is analyzed. Aside from the data sent by Threat Discovery Appliance, Threat Mitigator also checks the OfficeScan installation folder for the necessary virus/malware log files.</p> <p>For details, see Data Sources on page 5-2.</p>
Threat Management Services bandwidth allocation	<p>You can now set the upload and download limits for Threat Management Services to avoid disruptions to regular network traffic during the upload or download. For details, see Threat Management Services Registration on page 3-8.</p>

About Threat Mitigator

Threat Mitigator is a threat response solution that facilitates the elimination of threats detected on endpoints, including stealthy and zero-day internal threats. Threat Mitigator integrates with other Trend Micro products and services to provide the following protection types:

- Threat mitigation
- On-demand Scan

Threat Mitigation

Threat information received from data sources (such as **Threat Discovery Appliance** and **OfficeScan client**) prompts Threat Mitigator to issue mitigation tasks to the affected endpoints. Most mitigation tasks are carried out by **Threat Management Agent**, a program installed on an endpoint and managed by Threat Mitigator.

Threat mitigation tasks include:

Assessment

Threat Mitigator notifies Threat Management Agent to assess the endpoint after receiving a mitigation request from its data source. During assessment, the agent checks specific objects, processes, and network behavior connected to suspicious activity. Threat Mitigation then uses the Pattern-free Mitigation Engine and Template to stop suspicious processes, and disable and remove the targeted objects.

Post-assessment Cleanup

If the assessment confirms the presence of threats in the endpoint, Threat Management Agent runs post-assessment cleanup to eliminate threats. During cleanup, the agent leverages Trend Micro smart scan technology by using a lightweight pattern called Smart Scan Agent Pattern. This pattern is downloaded from Threat Mitigator. If the pattern is unable to determine the risk of a file, the agent sends a scan query to a **Smart Scan Server**.

A Smart Scan Server hosts the Smart Scan Pattern, which contains signatures not found in the Smart Scan Agent Pattern and checks whether the file is safe to access. A Smart Scan Server downloads the Smart Scan Pattern from the **Trend Micro ActiveUpdate server**.

Note: Set up a local Smart Scan Server to which agents send scan queries. If an agent cannot connect to the local scan server, it connects to the Global Smart Scan Server, a Trend Micro hosted service.

Threat Management Agent reports the cleanup results to Threat Mitigator. The results are stored in the threat event logs, which you can view from the product console.

Case Submission

Threat Mitigator integrates with **Threat Management Services**, a portal through which TrendLabs security experts monitor endpoints that require further mitigation.

When threats are not completely removed from the endpoint after running post-assessment cleanup, Threat Management Agent collects information about the threat and the infected endpoint and sends the information to Threat Mitigator. This prompts a security expert at TrendLabs to inform you about the threat and the infected endpoint, and to ask you to submit a case so that the threat can be analyzed. TrendLabs then issues a custom pattern through Threat Management Services to eliminate the threat.

Custom Pattern Deployment

Threat Mitigator downloads a custom pattern from Threat Management Services, deploys the pattern to the endpoint, and then notifies Threat Management Agent to run custom cleanup using the custom pattern. The agent reports the cleanup results back to Threat Mitigator.

On-demand Scan

On-demand Scan offers the same type of protection provided by endpoint security software (such as Trend Micro Internet Security™) but does not require software to be installed on the endpoint. Instead, the On-demand Scan program downloads a set of files from Threat Mitigator to a temporary folder in the endpoint. Scan results, logs, and other security information obtained during On-demand Scan are stored in this folder. Users can manually remove the folder if they no longer want to run the scan.

On-demand Scan can be launched on any endpoint on the network but is most useful on endpoints that do not have Threat Management Agent installed (also referred to as "agentless endpoints" in this document) and are connecting to the network for a limited period of time. For example, if you have guests or contractors who bring with them their own notebook computers, you can instruct them to run On-demand Scan instead of installing Threat Management Agent. On-demand Scan does not conflict with Trend Micro or third-party security software already installed on the endpoint.

On-demand Scan also leverages Trend Micro smart scan technology used during threat mitigation.

Threat Mitigator Integration

Threat Mitigator integrates with the following Trend Micro products and services:

- **Threat Discovery Appliance:** Acts as a data source for Threat Mitigator. Threat Discovery Appliance sends mitigation requests to Threat Mitigator after a threat is detected, and then notifies Threat Management Agent to run a mitigation task.
- **OfficeScan client:** Also acts as a data source for Threat Mitigator. Threat Management Agent monitors virus/malware detections logged by the OfficeScan client and then reports threats that have not been completely removed to Threat Mitigator. Threat Mitigator then notifies the agent to run a mitigation task.
- **Smart Scan Server:** A service hosted in-the-cloud that verifies potential threats detected during post-assessment cleanup or On-demand Scan. Endpoints connected to the corporate network send scan queries to a local Smart Scan Server if the risk of a file cannot be confirmed. Endpoints connect to the Global Smart Scan Server if the local scan server is unavailable.

- **Threat Management Services:** A security portal used by TrendLabs security experts for collecting threat samples from specific endpoints and issuing custom solutions to eliminate the threats.

The following diagram illustrates Threat Mitigator integration with other Trend Micro products and services:

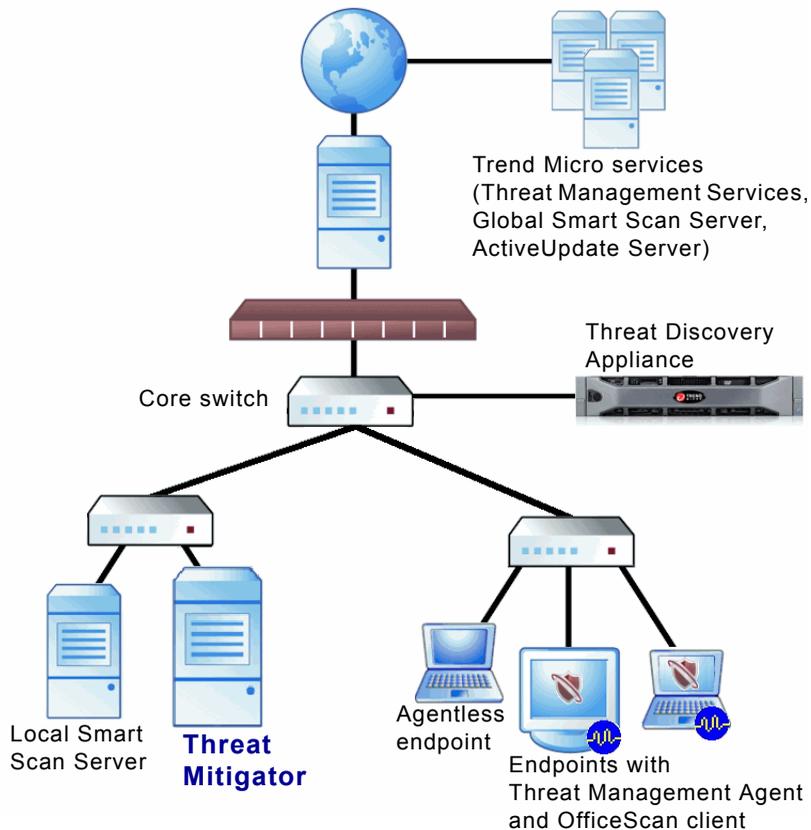


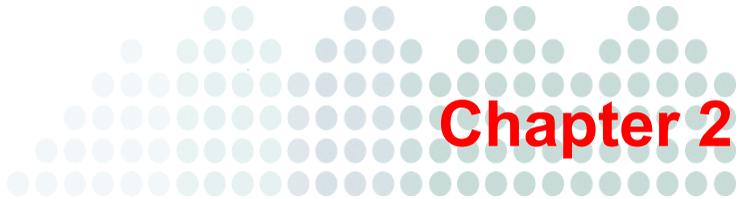
FIGURE 1-1. Threat Mitigator integration with other Trend Micro products and services

Key Features and Benefits

Threat Mitigator provides the following features and benefits:

TABLE 1-2. Threat Mitigator features and benefits

FEATURES	DESCRIPTIONS
Threat mitigation	Using information gathered from several data sources, Threat Mitigator issues mitigation tasks to Threat Management Agent, including assessment and cleanup. Security experts at TrendLabs issue custom patterns to be deployed to endpoints where initial cleanup was unsuccessful.
Rollback of cleanup tasks	During cleanup, Threat Management Agent may delete processes, files, and registry keys. If a false positive occurs, you can roll back the cleanup task and restore the deleted files and registry keys. Rollback is performed from the product console.
On-demand Scan	On-demand Scan provides protection to agentless endpoints, where routine threat mitigation tasks cannot be performed. On-demand Scan can also be launched on endpoints with agents installed.
Smart scan	Trend Micro smart scan technology is used during threat mitigation and On-demand Scan. This technology leverages lightweight patterns stored on the endpoint and in-the-cloud, reducing endpoint footprint while providing the same level of protection offered by conventional patterns.
Agent deployment	Deploy Threat Management Agent by using the Packager Tool or TMAgent Manager available from OfficeScan Plug-in Manager. For details about the agent deployment methods, see Agent Deployment Methods on page 4-3.



Installing or Upgrading Threat Mitigator

This chapter guides you through the Threat Mitigator installation and upgrade processes. It also provides instructions on how to uninstall the product.

This chapter includes the following topics:

- *Threat Mitigator System Requirements* on page 2-2
- *Pre-installation Guidelines* on page 2-3
- *Threat Mitigator Fresh Installation* on page 2-7
- *Threat Mitigator and Threat Management Agent Upgrades* on page 2-31
- *Threat Mitigator Uninstallation* on page 2-33

Threat Mitigator System Requirements

Threat Mitigator requires the following resources:

TABLE 2-1. Threat Mitigator system requirements

RESOURCES	REQUIREMENTS
Host machine	<ul style="list-style-type: none"> • Memory: 2GB recommended • Processor: Intel™ Pentium™ 4, 2.4GHz or faster • Available disk space: 10GB recommended
Virtual machine	<ul style="list-style-type: none"> • Memory: 512MB minimum • Processor: 2.4GHz or faster • Available disk space: 10GB recommended • Network adapter: At least one physical network adapter that connects to the network <p>If there is a separate management network in your environment, Threat Mitigator requires another physical network adapter that connects to the management network.</p>
Virtualization (minimum requirements)	<ul style="list-style-type: none"> • VMware™ ESX™/ESXi 4 with VMware vSphere™ Client • VMware ESX/ESXi 3.5 with VMware Infrastructure Client <p>For VMware system requirements, refer to the VMware Web site: http://www.vmware.com/products/vi/esx/</p> <hr/> <p>Tip: For better performance, Trend Micro recommends enabling Virtualization Technology in BIOS when installing VMware ESX/ESXi. Check if the BIOS of the host machine supports Virtualization Technology.</p> <hr/>

TABLE 2-1. Threat Mitigator system requirements (Continued)

RESOURCES	REQUIREMENTS
Browser	Microsoft™ Internet Explorer™ 6.0 or later to access the product console

Pre-installation Guidelines

Take note of the following before installing Threat Mitigator:

Threat Mitigator Placement

Install Threat Mitigator on the same network segment as Threat Discovery Appliance to facilitate threat mitigation. Additionally, position Threat Mitigator on a location that can reach endpoints.

Threat Mitigator Capacity

The following resources were used during the capacity tests performed by Trend Micro:

TABLE 2-2. Resources used in the Threat Mitigator capacity test

RESOURCE	SPECIFICATIONS
Threat Mitigator	Version 2.5 build 1177 (2.5.1177)
Host machine	Dell™ PowerEdge™ 2950
Virtual machine	<ul style="list-style-type: none"> • VMware ESX Server 3i version 3.5.0 Build 123629 • One virtual CPU • 512MB memory • Two hard disks (1.20GB for Threat Mitigator and 8GB for the Threat Mitigator database)

TABLE 2-2. Resources used in the Threat Mitigator capacity test (Continued)

RESOURCE	SPECIFICATIONS
Threat Management Agent	Version 2.7 build 1106 (2.7.1106) Note: This is the minimum version compatible with Threat Mitigator 2.5.1177. Newer agent versions should be compatible with Threat Mitigator 2.5.1177.

The capacity tests yielded the following results:

- Threat Mitigator can manage up to 4,700 Threat Management Agents. In extreme conditions, it can handle up to 4,000 agents simultaneously sending "heartbeat" messages. Heartbeat messages inform Threat Mitigator that a specific agent is up and running and can therefore run mitigation tasks. By default, all agents send heartbeat messages every 15 minutes and start to do so each time they start up (typically, as a result of the host computer starting up). It can be assumed that a large number of agents will not send heartbeat messages all at the same time because host computers do not start up at the same time.
- Threat Mitigator is not a CPU-bound application. Increasing the number of processors allotted for the product does not significantly improve its performance.

Network VirusWall Enforcer Installations

Trend Micro™ Network VirusWall™ Enforcer allows organizations to enforce security policies at the network layer. Network VirusWall Enforcer can identify infected endpoints and deliver cleanup services to these endpoints. It can also isolate endpoints with software vulnerabilities, endpoints without adequate anti-malware protection, and endpoints that violate network usage policies.

Some Network VirusWall Enforcer features (such as endpoint cleanup) are also available in Threat Mitigator. To avoid feature conflicts and to ensure that both products run simultaneously without problems, verify the items listed in this topic.

Note: Refer to the Network VirusWall Enforcer documentation for information on configuring settings for this product.

1. Use Network VirusWall Enforcer 2.0 with Service Pack 1 or later. Upgrade Network VirusWall Enforcer if you have an earlier version running.
2. Ensure that the threat mitigation option in Network VirusWall Enforcer policies has been disabled.
3. Do not run manual or scheduled updates of the following Network VirusWall Enforcer components used for threat mitigation:
 - Forensic Cleanup Engine
 - Forensic Cleanup Template
 - Anti-rootkit Driver
4. Add the Threat Mitigator IP address to the Global Endpoint Exception List in Network VirusWall Enforcer.

Note: To configure the Threat Mitigator IP address, see [Phase 3: Configuring the IP Address](#) on page 2-27 and [IP Address Settings](#) on page 8-8.

Integration with Other Trend Micro Products

For seamless integration with other Trend Micro products, ensure that the products run the following versions:

TABLE 2-1. Minimum and recommended versions of Trend Micro products

TREND MICRO PRODUCT	VERSION
Threat Discovery Appliance	<ul style="list-style-type: none">• 2.5 R2 (recommended)• 2.0 (minimum)
OfficeScan client	<ul style="list-style-type: none">• 10.0 (minimum)
Smart Scan Server	<ul style="list-style-type: none">• 1.1 Service Pack 1 (recommended)• 1.0 (minimum)

Threat Mitigator Fresh Installation

Threat Mitigator fresh installation involves the following tasks:

1. *Setting Up the VMware Server* on page 2-7
2. *Setting Up the VMware Client* on page 2-8
3. *Setting Up Threat Mitigator* on page 2-10

Note: If you are upgrading Threat Mitigator, see *Threat Mitigator and Threat Management Agent Upgrades* on page 2-31.

Setting Up the VMware Server

Threat Mitigator can be installed on a VMware ESX or ESXi server. The VMware server runs on a host machine with the specifications listed in *Host machine* on page 2-2.

The VMware ESX/ESXi server is not included in the Threat Mitigator installation package. Visit the VMware Web site for information on how to obtain the product.

To set up the VMware server:

1. Prepare the host machine and ensure it is connected to the network.
2. Install the VMware server on the host machine. VMware automatically detects the physical ports and assigns the ports to a designated virtual switch.
3. Connect the router to the VMware host machine.
4. Record the HTTPS URL (`https://<ESX_IP_address>`) of the VMware server. You will use the URL when you set up the VMware client.

Setting Up the VMware Client

Use the VMware client that comes with the VMware ESX/ESXi server to install and manage applications (such as Threat Mitigator) on the VMware server. Install the client on another computer that can connect to the VMware server.

If you have installed VMware ESX/ESXi 4.0, set up the **VMware vSphere Client**.

If you have installed VMware ESX/ESXi 3.5, set up the **VMware Infrastructure Client**.

To set up the VMware client:

1. On the computer that will host the VMware client, open a browser window and type the HTTPS URL of the VMware server.
2. For VMware ESX/ESXi 4.0, click **Download vSphere Client**.

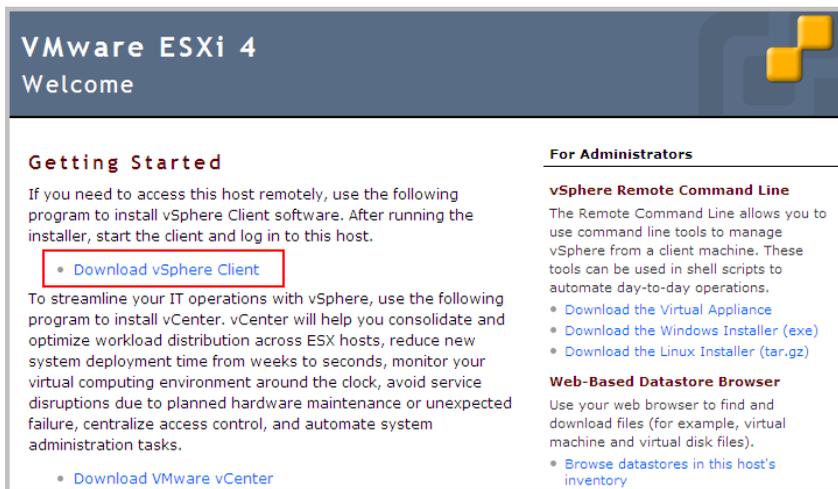


FIGURE 2-1. VMware ESX/ESXi 4.0 Welcome page

For VMware ESX/ESXi 3.5, click **Download VMware Infrastructure Client**.



VMware ESX Server 3
Welcome

Getting Started

If you need to access this host remotely, use the following program to install VMware Infrastructure client software. After running the installer, start the client and log in to this host.

- [Download VMware Infrastructure Client](#)

To streamline your IT operations with VMware Infrastructure, use the following program to install VirtualCenter Server. VirtualCenter Server will help you consolidate and optimize workload distribution across ESX Server hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.

- [Download VMware VirtualCenter Server](#)

If you need more help, please refer to our documentation library:

For Administrators

VMware Infrastructure Web Access
VMware Infrastructure Web Access streamlines remote desktop deployment by allowing you to organize and share virtual machines using ordinary web browser URLs.

- [Log in to Web Access](#)

Web-Based Datastore Browser
Use your web browser to find and download files (for example, virtual machine and virtual disk files).

- [Browse datastores in this host's inventory](#)

ESX Server Scripted Installer
This browser-based utility allows you to automate host provisioning.

FIGURE 2-2. VMware ESX/ESXi 3.5 Welcome page

3. Follow the on-screen instructions to install the client.

Setting Up Threat Mitigator

Setting up Threat Mitigator involves the following phases:

- *Phase 1: Preparing the Threat Mitigator Installation Package* on page 2-10
- *Phase 2: Installing Threat Mitigator* on page 2-11
- *Phase 3: Configuring the IP Address* on page 2-27

Phase 1: Preparing the Threat Mitigator Installation Package

The Threat Mitigator installation package is available for download from the Trend Micro Web site. You can also obtain the installation package from your Trend Micro representative.

Copy the package to the computer where you installed the VMware client (VMware vSphere Client or VMware Infrastructure Client). The package includes:

- A file in Open Virtualization Format (.ovf) format
- Two files in Virtual Machine Disk (.vmdk) format

Phase 2: Installing Threat Mitigator

If you have installed VMware ESX/ESXi 4.0, use the **VMware vSphere Client** to install Threat Mitigator.

If you have installed VMware ESX/ESXi 3.5, use the **VMware Infrastructure Client**. For details, see *To set up Threat Mitigator from the VMware Infrastructure Client*: on page 2-18.

To install Threat Mitigator from the VMware vSphere Client:

Part 1: Deploying the .ovf file

1. Open the vSphere Client and then type the logon credentials for the VMware server.



FIGURE 2-3. vSphere Client logon page

2. On the client's main screen, click **Inventory**.

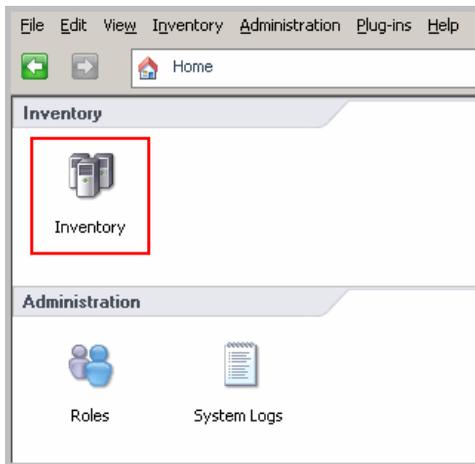


FIGURE 2-4. vSphere Client main screen

3. Click **File > Deploy OVF Template** from the main menu.
4. Select **Deploy from file**, browse to the location of the Threat Mitigator `.ovf` file, and then click **Next**.

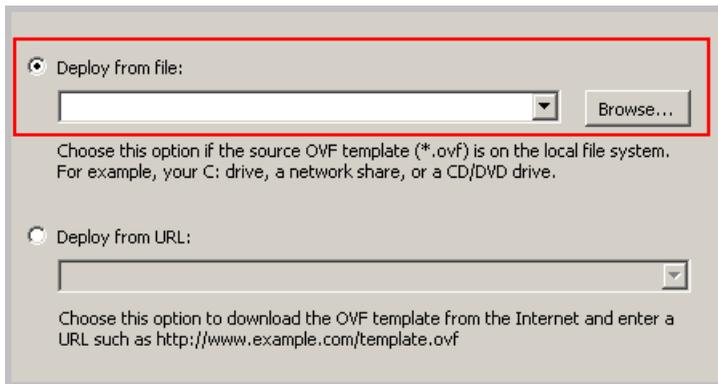


FIGURE 2-5. Deploy OVF Template screen

5. Confirm the size of the file and then click **Next**.
6. Specify a name for Threat Mitigator. The default name is the `.ovf` file name without the file extension.
7. If prompted, specify which network in the vSphere inventory will be used for the virtual machines in the `.ovf` file.
8. Review the settings and then click **Finish** if all settings are correct.

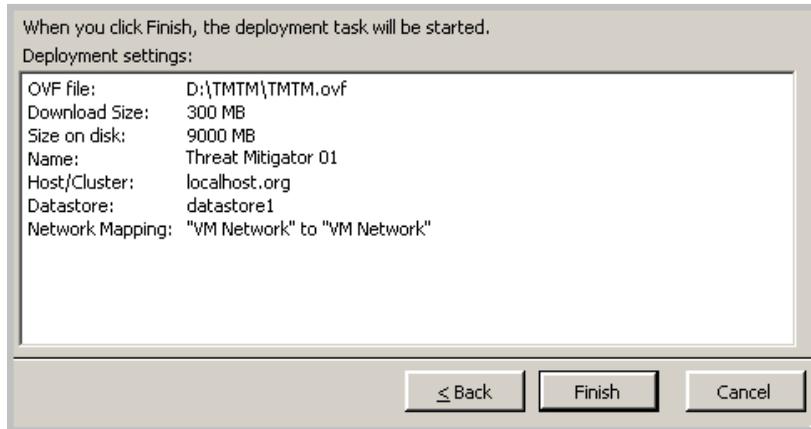


FIGURE 2-6. Ready to Complete screen

Threat Mitigator starts to install to the VMware server.

Part 2: Configuring network adapter settings

1. After Threat Mitigator installs successfully, access the vSphere Client, right-click Threat Mitigator from the menu on the left, and then click **Edit Settings**.

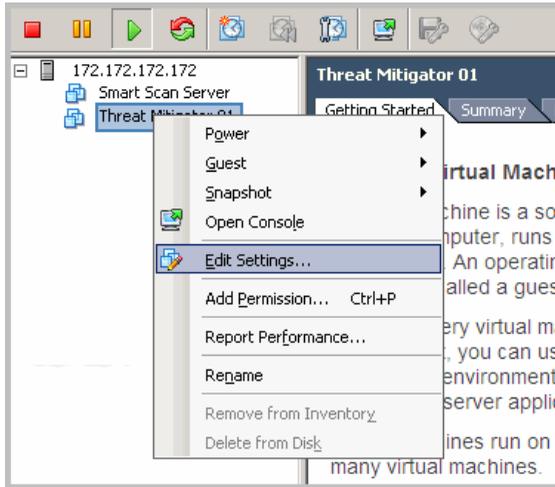


FIGURE 2-7. vSphere Client screen showing virtual machines

2. On the **Hardware** tab, select **Network adapter 1** and ensure that the **Connect at power on** option is enabled.

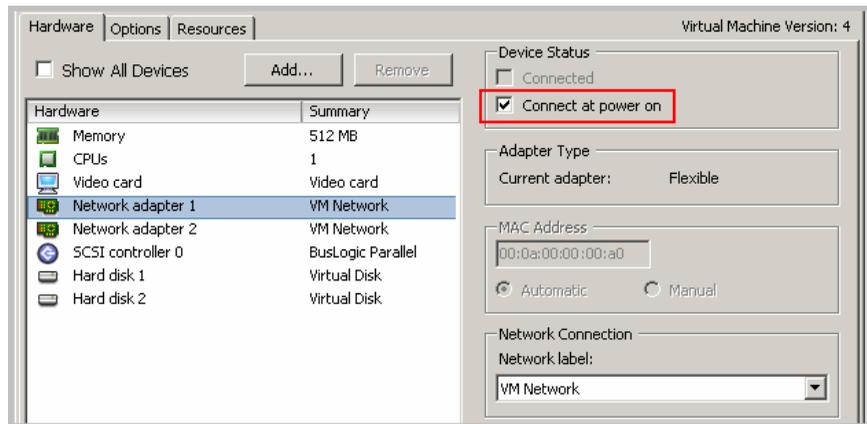


FIGURE 2-8. Network adapter 1 settings

3. If there is a separate management network in your environment:
 - a. Select **Network adapter 2**, go to the **Network Connection** section, and then select **Management Network**.
 - b. Ensure that the **Connected** and **Connected at power on** options are enabled.

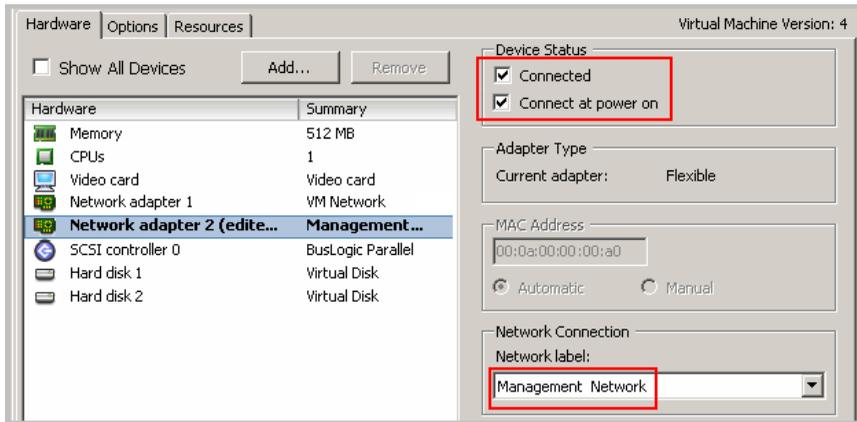


FIGURE 2-9. Network adapter 2 settings

4. Click **OK**.

Part 3: Powering on Threat Mitigator

1. Right-click Threat Mitigator from the menu on the left, and then select **Power > Power On**. It may take a few minutes to start Threat Mitigator.

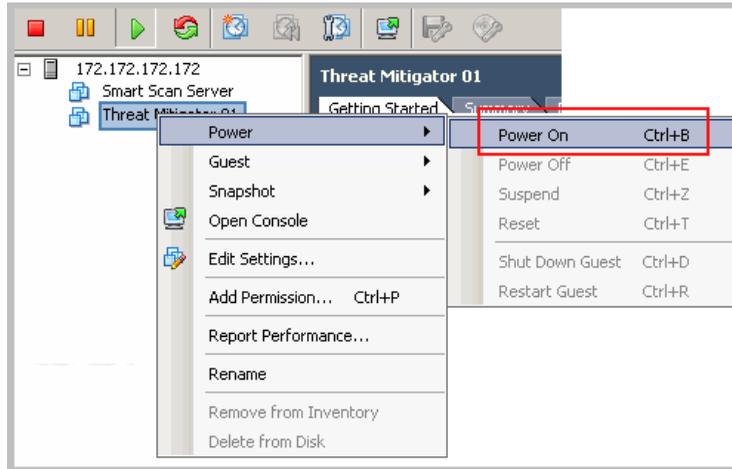


FIGURE 2-10. Power On option

2. To check the startup progress, right-click Threat Mitigator from the menu on the left, and then select **Open Console**. A command line interface displays.

```

Booting the TrendMicro Common Platform 1000...

[ 5.381178] sda: assuming drive cache: write through
[ 5.381178] sda: assuming drive cache: write through
[ 5.401457] sdb: assuming drive cache: write through
[ 5.401618] sdb: assuming drive cache: write through

Please type 'r' to enter rescue mode, waiting 5 seconds
5 seconds left..
4 seconds left..
3 seconds left..
-

```

FIGURE 2-11. Threat Mitigator startup

When startup is complete, the preconfiguration console's Welcome screen displays. Configure the Threat Mitigator IP address from the console. For details, see [Phase 3: Configuring the IP Address](#) on page 2-27.

To set up Threat Mitigator from the VMware Infrastructure Client:

Part 1: Deploying the .ovf file

1. Open the VMware Infrastructure Client and then type the logon credentials for the VMware server.



FIGURE 2-12. VMware Infrastructure Client logon page

2. On the **Getting Started** tab, click **Import a virtual appliance**.



FIGURE 2-13. VMware Infrastructure Client main screen

3. Select **Import from file**, browse to the location of the Threat Mitigator .ovf file, and then click **Next**.

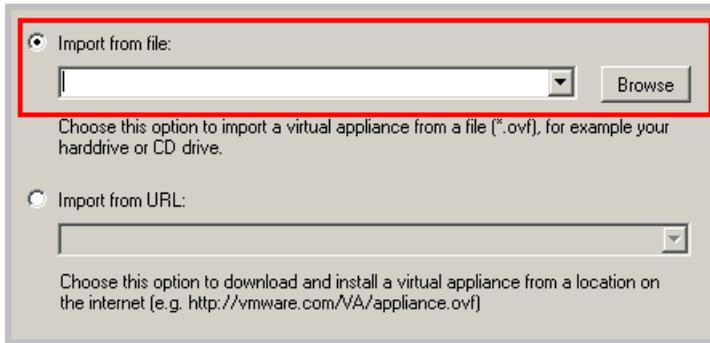


FIGURE 2-14. Import Location screen

4. Confirm the size of the file and then click **Next**.
5. Specify a name for Threat Mitigator. The default name is the .ovf file name without the file extension.
6. If prompted, specify which network in the VirtualCenter Server inventory corresponds to the networks specified for the virtual machines in the .ovf file.

7. Review the settings and then click **Finish** if all settings are correct.

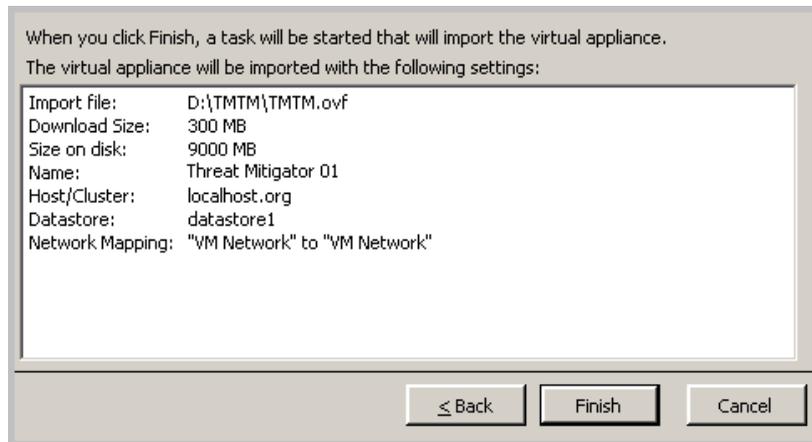


FIGURE 2-15. Ready to Complete Virtual Appliance Import screen

Threat Mitigator starts to install to the VMware server.

Part 2: Configuring network adapter settings

1. After Threat Mitigator installs successfully, access the VMware Infrastructure Client, right-click Threat Mitigator from the menu on the left, and then click **Edit Settings**.

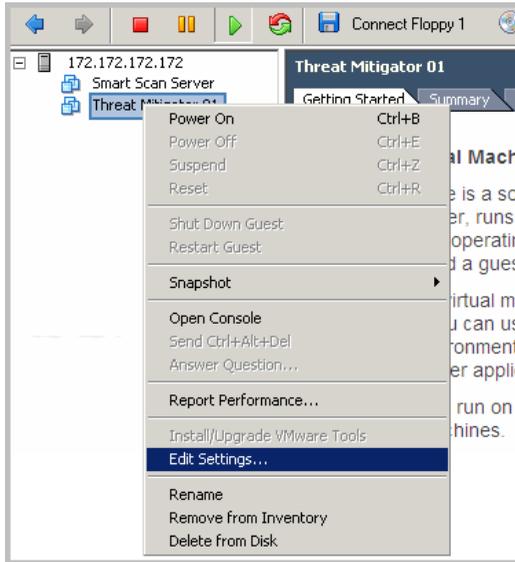


FIGURE 2-16. VMware Infrastructure Client screen showing virtual machines

2. On the **Hardware** tab, select **Network Adapter 1** and ensure that the **Connect at power on** option is enabled.

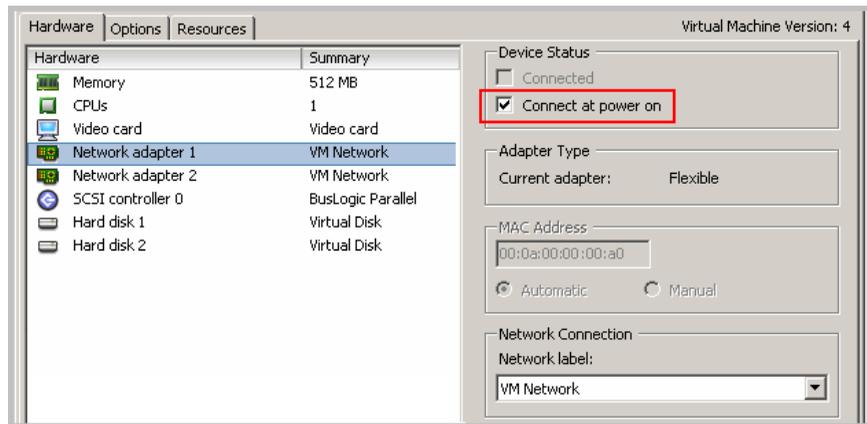


FIGURE 2-17. Network adapter 1 settings

3. If there is a separate management network in your environment:
 - a. Select **Network adapter 2**, go to the **Network Connection** section, and then select **Management Network**.
 - b. Ensure that the **Connected** and **Connected at power on** options are enabled.

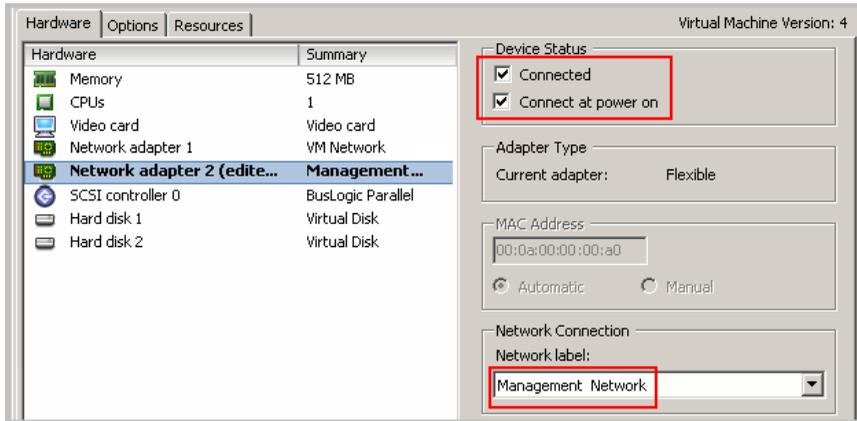


FIGURE 2-18. Network adapter 2 settings

4. Click **OK**.

Part 3: Powering on Threat Mitigator

1. Right-click Threat Mitigator from the menu on the left, and then select **Power On**. It may take a few minutes to start Threat Mitigator.

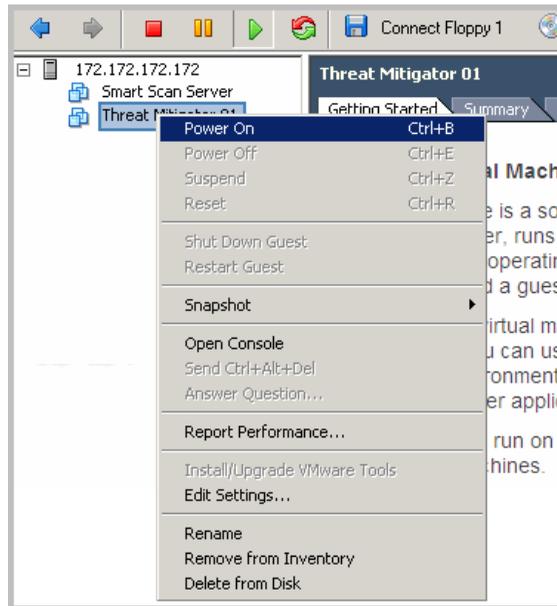


FIGURE 2-19. Power On option

2. To check the startup progress, right-click Threat Mitigator from the menu on the left, and then select **Open Console**. A command line interface displays.

```
Booting the TrendMicro Common Platform 1000...

[ 5.381178] sda: assuming drive cache: write through
[ 5.381178] sda: assuming drive cache: write through
[ 5.401457] sdb: assuming drive cache: write through
[ 5.401618] sdb: assuming drive cache: write through

Please type 'r' to enter rescue mode, waiting 5 seconds
5 seconds left..
4 seconds left..
3 seconds left..

-
```

FIGURE 2-20. Threat Mitigator startup

When startup is complete, the preconfiguration console's Welcome screen displays. Configure the Threat Mitigator IP address from the console. For details, see [Phase 3: Configuring the IP Address](#) on page 2-27.

Phase 3: Configuring the IP Address

Assign a static IP address to Threat Mitigator from the preconfiguration console. The preconfiguration console is a terminal communications program used for configuring initial settings necessary for the product to be fully functional. The console displays after you power on Threat Mitigator from the VMware client.

Threat Mitigator, the VMware ESX/ESXi server, and Smart Scan Server (if one has been set up) require unique IP addresses. Check the IP addresses of the VMware ESX/ESXi server and Smart Scan Server and ensure that none of these IP addresses is assigned to Threat Mitigator.

Note: If you have set up Network VirusWall Enforcer, add the Threat Mitigator IP address to the Global Endpoint Exception List in Network VirusWall Enforcer. Refer to the Network VirusWall Enforcer documentation for the procedure.

For other guidelines related to Network VirusWall Enforcer installations, see [Network VirusWall Enforcer Installations](#) on page 2-5.

To assign a static IP address to Threat Mitigator:

1. On the Welcome screen, type the logon user name and password. Press the **Tab**, **Up**, or **Down** key to navigate between fields.

```

=====Welcome to Trend Micro Threat Mitigator=====

*****
* Trend Micro Threat Mitigator Preconfiguration *
*                               *
*****2.50.1096*****

User name:admin
Password:  _

                                OK

-----
<UP>,<DOWN>,<TAB>:Change field. <ENTER>:Select field. <Ctrl+R>:Refresh screen.

```

FIGURE 2-21. Welcome screen

The default logon credentials are as follows:

- User name: admin
- Password: admin

Tip: Change the password after logging on to the product console. For details, see *Product Console Password* on page 3-6.

2. Press **Enter** to log on.
3. Type **1** to highlight the **Device Settings** option and then press **Enter**.



FIGURE 2-22. Main Menu screen with Device Settings highlighted

4. On the Device Settings screen, type the following:
 - Host name
 - IP address
 - Subnet mask
 - Default gateway
 - Primary DNS server
 - Secondary DNS server
 - IP address and subnet mark of the management interface (if there is a separate management network in your environment)

```
=====Device Settings=====
Host Name
Host name: TMTM

Configure Data Interface
IP address: 10.10.10.0
Subnet mask: 255.255.255.255
Default gateway: 10.10.10.100
Primary DNS server: 10.10.10.10
Secondary DNS server: 10.10.100.10

[*] Enable Separate Management Interface [NIC#2]
IP address: 192.192.192.192
Subnet mask: 255.255.255.0_

Return to the Main menu

<UP>, <DOWN>, <TAB>: Change field. <SPACEBAR>: Change value. <ENTER>: Select field.
```

FIGURE 2-23. Device Settings screen

5. Navigate to **Return to main menu** and then press **Enter**.

6. Type **6** to highlight the **Save and Log Off** option and then press **Enter**.



FIGURE 2-24. Main Menu screen with Save and Log Off highlighted

Note: After configuring the IP address, you can change it from the product console. For details, see [IP Address Settings](#) on page 8-8.

Threat Mitigator and Threat Management Agent Upgrades

This Threat Mitigator version supports both version and build upgrades.

- **Version upgrade:** If you are running an earlier Threat Mitigator version, perform the steps in *Setting Up Threat Mitigator* on page 2-10 to upgrade to this version.
- **Build upgrade:** If you have installed an earlier build for this product version, you can upgrade to a newer build by updating certain Threat Mitigator components. The upgrade procedure is discussed in this topic.

After Threat Mitigator upgrades, the Threat Management Agents that connect to Threat Mitigator automatically upgrade. Users may or may not need to restart the endpoint after the agent upgrades, depending on the status of agent components. Instruct users to restart the endpoint when prompted.

To upgrade successfully, ensure that Threat Mitigator and Threat Management Agents satisfy the requirements specified in the following topics:

- *Threat Mitigator System Requirements* on page 2-2
- *Agent System Requirements* on page 4-2

Note: To perform Threat Mitigator fresh installation, see *Threat Mitigator Fresh Installation* on page 2-7. To perform Threat Management Agent fresh installation, see *Deploying Threat Management Agents* on page 4-1.

To perform a build upgrade:

1. Log on to the Threat Mitigator console.
2. Back up the product configurations by navigating to **Administration > Backup**.

Note: If you encounter problems upgrading Threat Mitigator, use the backup file to restore configurations.

3. Navigate to **Updates > Manual**.
4. Select the following components:
 - Damage Cleanup Engine
 - Threat Management Agent
 - System Clean and Forensic Module
 - Program
5. Click **Update**.
6. Click **Reset** when prompted.

Threat Mitigator upgrades. Agents that connect to Threat Mitigator automatically upgrade.

Note: After the agent upgrades, users may or may not need to restart the endpoint, depending on the status of some agent components. Instruct users to restart the endpoint when prompted.

7. Verify that the upgrades were successful.
 - a. Log on to the Threat Mitigator console.
 - b. On the banner section of the screen, select **About** from the dropdown box and then verify the build number.
 - c. On the endpoint's system tray, right-click the Threat Management Agent icon, click **About**, and then verify the program version.

Threat Mitigator Uninstallation

To remove Threat Mitigator, follow the procedures in the following topics:

Unregistering Threat Mitigator from Threat Discovery Appliance

Ensure that you remove all registered Threat Discovery Appliances before you uninstall Threat Mitigator.

To unregister Threat Mitigator from Threat Discovery Appliance:

1. On the Threat Discovery Appliance console, click **Mitigation > Mitigation Settings** in the main menu. The Mitigation Settings screen appears.
2. Under **Registered Mitigation Devices**, select the Threat Mitigator IP address or sever name.
3. Click **Delete**.

Uninstalling Threat Management Agent from Endpoints

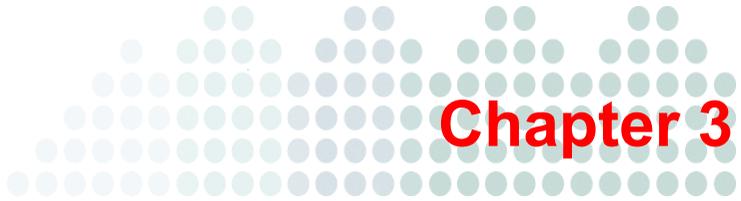
Uninstall the agent from the Control Panel or by creating a logon script. For details, see [Agent Uninstallation](#) on page 4-22.

Uninstalling Threat Mitigator

Uninstall Threat Mitigator from the VMware ESX server.

To uninstall Threat Mitigator:

1. Run the vSphere Client or the VMware Infrastructure Client.
2. Log on to the VMware ESX server.
3. Select Threat Mitigator from the list of virtual machines.
4. Power off the virtual machine.
 - For vSphere Client, click **Inventory > Virtual Machine > Power > Power Off**.
 - For VMware Infrastructure Client, click **Inventory > Virtual Machine > Power Off**.
5. Click **Inventory > Virtual Machine > Delete from Disk**.



Getting Started

This chapter discusses settings you need to configure after installing Threat Mitigator.

This chapter contains the following topics:

- *The Product Console* on page 3-2
- *Product License and Activation Code* on page 3-7
- *Threat Management Services Registration* on page 3-8
- *Component Updates* on page 3-10
- *Proxy Settings* on page 3-16
- *System Time* on page 3-7
- *Smart Scan Server Setup* on page 3-17

The Product Console

Threat Mitigator provides a built-in Web-based product console through which you can configure product settings. Access the product console from any computer on the same network as the VMware server.

To log on to the product console:

1. Open Internet Explorer and type the product console URL.

`https://<IP address>/TMAdmin`

Tip: For convenience, bookmark this URL in the Web browser.

2. Type the logon credentials and click **Log On**. The default credentials are:

- User name: admin
- Password: admin

The product console opens. The console consists of the banner, the main menu bar, and the main content window.

Note: The default system timeout is 600 seconds (10 minutes).

Product Console Banner

The product console banner on top of the screen displays the name of the product, contains the **Setup Guide** and **Log Off** links, and provides a drop-down menu listing several navigational options.

Click **Setup Guide** to display the steps for initial configuration of the product settings. Click **Log Off** from within any screen at any time to log off from the console and return to the logon screen.

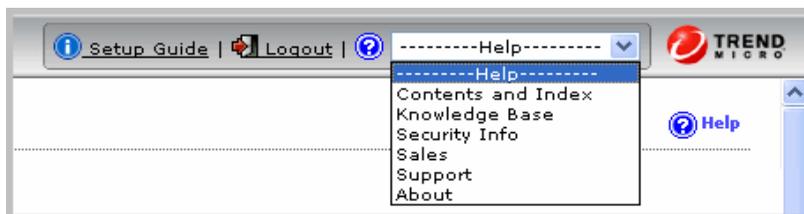


FIGURE 3-1. Product console banner

The navigational options from the drop-down menu are as follows:

TABLE 3-1. Navigational options in the top banner drop down menu

OPTIONS	DESCRIPTIONS
Contents and Index	Opens the Threat Mitigator Help
Knowledge Base	Opens the search page of the Trend Micro Knowledge Base
Security Info	Opens the Trend Micro Security Information page, where you can get the latest Trend Micro advisories on malware, spyware/grayware, and other security issues
Sales	Opens the Trend Micro sales Web page, where you can contact your regional sales representative
Support	Provides information on how to get online, telephone, and email support

TABLE 3-1. Navigational options in the top banner drop down menu (Continued)

OPTIONS	DESCRIPTIONS
About	Provides information about Threat Mitigator, including the product version, build number, service pack version, and hot fix number

Main Menu Bar

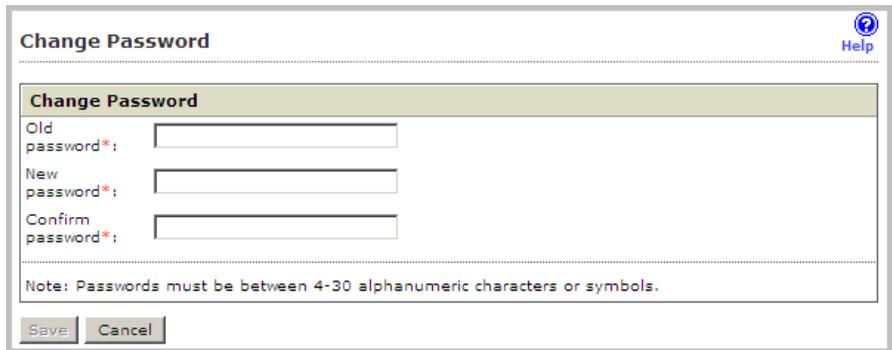
The main menu bar comprises of several menu items that allow you to configure product settings. An arrow before a menu item indicates that the menu item has several sub-menus.

**FIGURE 3-2. The main menu bar**

Main Content Window

The main content window displays information relevant to the menu item selected in the main menu bar and allows you to configure settings or issue tasks.

Click the question mark icon  at the top right corner of the window to access context-sensitive help.



Change Password  Help

Change Password

Old password*:

New password*:

Confirm password*:

Note: Passwords must be between 4-30 alphanumeric characters or symbols.

Save Cancel

FIGURE 3-3. The main content window showing password settings

Product Console Password

The default console password is `admin`. For improved security, Trend Micro recommends changing the password after logging on for the first time and periodically thereafter.

Passwords must contain 4 to 30 alphanumeric characters (such as 0-9, a-z, A-Z). The following symbols are also accepted:

`! \ " # $ % & ' () * + , - . / : ; < = > ? @ [] ^ _ ` { | } ~`

The following are guidelines for creating a safe password:

- Avoid words found in the dictionary.
- Intentionally misspell words.
- Use phrases or combine words.
- Use both uppercase and lowercase letters.

If you lose the password, there is no way to recover it. Contact your support provider for assistance in resetting the password.

To change the product console password:

PATH: ADMINISTRATION > CHANGE PASSWORD

1. Type the current password.
2. Type the new password and confirm it.
3. Click **Save**.

Product License and Activation Code

To use the functionality of Threat Mitigator, obtain an Activation Code and then activate the license.

You can activate or renew the Threat Mitigator license in the Product License screen.

To manage the product license:

PATH: ADMINISTRATION > PRODUCT LICENSE

1. Click **New Activation Code**.
2. Type the Activation Code in the screen that opens and click **Save**.
3. Read and then agree to the License Agreement, which only displays when activating the license for the first time.
4. Enable Threat Management Services when prompted. For details, see [Threat Management Services Registration](#) on page 3-8.
5. Back in the Product License screen, click **Update Information** to refresh the screen with the new license details. This screen also provides a link to the Trend Micro Web site where you can view detailed information about your license.

System Time

Threat Mitigator receives threat information from its data sources (such as Threat Discovery Appliance and OfficeScan) and integrates with other Trend Micro products and services to perform threat mitigation. If the system times in Threat Mitigator and the products and services it integrates with are not synchronized, information may become unreliable and cause confusion. Configure Threat Mitigator to synchronize its system time with a Network Time Protocol (NTP) server to avoid these issues.

To configure system time settings:

PATH: ADMINISTRATION > DEVICE CONFIGURATION > SYSTEM TIME

1. Type the NTP server address.
2. Click **Synchronize Now**.

Note: If the synchronization was unsuccessful, Threat Mitigator retries the synchronization twice, at 20-second intervals. This event is recorded in the system logs. For details about system logs, see [System Logs](#) on page 7-13.

3. Select the time zone to use.
4. Click **Save**.

Threat Management Services Registration

Threat Management Services is a security portal through which Trend Micro security experts can receive threat information from registered products, and then issue targeted security solutions and reports to the products. Register Threat Mitigator to Threat Management Services to respond to threats in a timely manner and receive up-to-date information about the latest and emerging threats.

Threat Management Services works with Threat Mitigator by:

- Analyzing threats that have not been eliminated completely
- Deploying solutions to infected endpoints through Threat Mitigator to eliminate the threats
- Providing incident reports detailing malicious behaviors and the chain of events that led to endpoint infections. Reports also contain Trend Micro recommended actions.

Threat Mitigator sends heartbeat messages to Threat Management Services periodically. A heartbeat message informs Threat Management Services that Threat Mitigator is up and running and can therefore initiate threat mitigation tasks.

Before registering Threat Mitigator to Threat Management Services, ensure that you have obtained the required information for registration. Contact your Trend Micro representative or support provider to obtain the registration information, which includes:

- Name or IP address of the server hosting the services
- Server authentication credentials

Note: Configure proxy settings if a proxy server is used to connect to Threat Management Services. For details, see [Proxy Settings](#) on page 3-16.

To register Threat Mitigator to Threat Management Services:

PATH: SERVICES > THREAT MANAGEMENT SERVICES

1. Select **Send Threat Mitigator data and logs to Trend Micro through Threat Management Services**.
2. Type the server name or IP address of the server to which to send logs.
3. Select the protocol. You can select either **SSH** or **SSL**.
4. Select the frequency of log transmissions.
5. Type the server name or IP address of the server to which to send status information.
6. Specify the upload or download bandwidth.
7. Type the user name and password you used to log on to Threat Management Services.
8. Type the email address you used to register to Threat Management Services.
9. To check whether Threat Mitigator can connect to Threat Management Services based on the settings you specified, click **Test Connection**.
10. Click **Save** if the test connection was successful.

Component Updates

Threat Mitigator uses various components for threat mitigation and On-demand Scan. Threat Mitigator downloads components from its update source, which is the Trend Micro ActiveUpdate server by default. Update components on demand or configure an update schedule.

Threat Mitigator Components

Threat Mitigator uses the following components:

TABLE 3-2. Threat Mitigator components

COMPONENT	DESCRIPTION
Pattern-free Mitigation Engine	Scans and removes threats detected by Threat Discovery Appliance
Pattern-free Mitigation Template	Used by the Pattern-free Mitigation Engine to identify potential threats detected by Trend Micro™ Threat Discovery Appliance
System Clean and Forensic Module	The module that: <ul style="list-style-type: none"> • Scans specifically for active malware to reduce scan time • Provides enhanced detection and cleanup to address complicated threats • Checks and compares scan results, and performs file recovery
Virus Scan Engine	Works with the Smart Scan Agent Pattern to identify the latest virus/malware and mixed threat attacks
Smart Scan Agent Pattern	A lightweight pattern that contains information to identify the latest virus/malware and mixed threat attacks. This pattern is used with the Smart Scan Pattern hosted on a Smart Scan Server to provide the same level of protection offered by conventional anti-malware patterns.

TABLE 3-2. Threat Mitigator components (Continued)

COMPONENT	DESCRIPTION
Damage Cleanup Engine	Scans and removes Trojans and Trojan processes
Damage Cleanup Template	Used by the Damage Cleanup Engine to identify Trojan files and processes so the engine can eliminate them
Anti-rootkit Driver	Used by the Trend Micro scan engines to prevent any potential redirection by rootkits
Programs/Other Components	
Threat Management Agent	The program in the endpoint that: <ul style="list-style-type: none"> • Performs threat mitigation • Monitors endpoint security risk logs • Collects logs and suspicious file samples
Antivirus Product Detection Engine	Detects antivirus products currently installed in the endpoint
Program Version	The program software currently installed

Update Process

To update components successfully, perform the following tasks:

1. Configure the update source. For details, see [Update Source](#) on page 3-13.
2. If a proxy server is used to connect to the update source, configure proxy settings. For details, see [Proxy Settings](#) on page 3-16.
3. Perform a manual update. For details, see [Manual Updates](#) on page 3-14.
4. Configure an update schedule. For details, see [Scheduled Updates](#) on page 3-15.

Network VirusWall Enforcer Components

If you have set up Network VirusWall Enforcer, do not run manual or scheduled updates of the following components from the Network VirusWall Enforcer product console to avoid feature conflicts:

- Forensic Cleanup Engine
- Forensic Cleanup Template
- Anti-rootkit Driver

Note: For other guidelines related to Network VirusWall Enforcer installations, see [Network VirusWall Enforcer Installations](#) on page 2-5.

Update Source

Threat Mitigator downloads components from the Trend Micro ActiveUpdate server, the default update source. However, you can configure Threat Mitigator to download components from another update source.

To configure the update source:

PATH: UPDATES > SOURCE

1. Select an update source.
 - If you choose **ActiveUpdate server**, ensure that Threat Mitigator has Internet connection and, if you are using a proxy server, test if Internet connection can be established using the proxy settings. For details, see [Proxy Settings](#) on page 3-16.
 - If you choose a custom update source, set up the appropriate environment and update resources for this update source. Also ensure that there is a functional connection between Threat Mitigator and this update source. If you need assistance setting up an update source, contact your support provider.
2. Enable Threat Mitigator to retry an update if it was unsuccessful.
 - Specify the number of retry attempts and the retry interval.
 - Specify the download timeout. If components are not downloaded within the specified amount of time, the update is considered unsuccessful.
3. Click **Save**.

Update Methods

Threat Mitigator provides two methods for updating components:

- **Manual Update:** When an update is critical, perform manual update so Threat Mitigator can obtain the updates immediately. For details, see [Manual Updates](#) on page 3-14.
- **Scheduled Update:** Threat Mitigator automatically checks the update source at the frequency you specify. For details, see [Scheduled Updates](#) on page 3-15.

Manual Updates

Perform a manual update after installing or upgrading Threat Mitigator and when an update is critical.

To perform a manual update:

PATH: UPDATES > MANUAL

1. Select the components to update. To check if a component requires an update, compare a component's current version with the version available on the update source.
2. Click **Update**.

Scheduled Updates

Configure Threat Mitigator to regularly check its update source and automatically download any available updates. Scheduled update relieves you of the task of manually keeping Threat Mitigator up-to-date.

Tip: Schedule updates during off-peak hours.

To configure scheduled updates:

PATH: UPDATES > SCHEDULED

1. Select the components to update when scheduled update runs.
2. Specify the update schedule.

TABLE 3-3. Update schedules

OPTION	FREQUENCY	DESCRIPTION
Minutes, every:	Every X minutes	Runs within the minute you specify, at the start time
Hours, every:	Every X hours	Runs within the hour you specify, at the start time
Days, every:	Every X days	Runs within the day you specify, at the start time
Weekly, every:	Week, on X day	Runs weekly, on the day you specify, at the start time

3. Click **Save**.

Proxy Settings

Configure Threat Mitigator to use the proxy settings when performing the following:

- Connecting to Threat Management Services
- Downloading updates from the Trend Micro ActiveUpdate server or another update source

To configure proxy settings:

PATH: ADMINISTRATION > NETWORK CONFIGURATION > PROXY SETTINGS

1. Select **Use a proxy server for pattern, engine, and license updates**.
2. Select the proxy protocol.
3. Type the server name or IP address and the port number.
4. If your proxy server needs authentication, type the user name and password in the fields provided.
5. Click **Save**.

Smart Scan Server Setup

Threat Mitigator leverages Trend Micro smart scan technology during routine mitigation tasks and On-demand Scan. Smart scan technology is a next-generation, in-the-cloud based endpoint protection solution. At the core of this solution is an advanced scanning architecture that leverages threat signatures stored in-the-cloud.

Threat Mitigator downloads and updates a lightweight pattern called Smart Scan Agent Pattern. If this pattern is unable to determine the risk of a file during mitigation or On-demand Scan, a scan query is sent to a cloud-based server called Smart Scan Server.

A Smart Scan Server hosts the Smart Scan Pattern, which contains signatures not found in the Smart Scan Agent Pattern and checks whether the file is safe to access. A Smart Scan Server downloads and updates the Smart Scan Pattern from the Trend Micro ActiveUpdate server.

Smart Scan Server Installation

Install Smart Scan Server on a VMware server. Only one Smart Scan Server can be used in this Threat Mitigator version. For installation instructions and requirements, refer to the Trend Micro Smart Scan Server Getting Started Guide.

Note: For information on the Smart Scan Server versions compatible with Threat Mitigator, see *Integration with Other Trend Micro Products* on page 2-6.

Smart Scan Server, Threat Mitigator, and the VMware ESX/ESXi server (which hosts the Smart Scan Server and Threat Mitigator) require unique IP addresses. Check the IP addresses of the VMware ESX/ESXi server and Threat Mitigator and ensure that none of these IP addresses is assigned to Smart Scan Server.

If you have previously installed a Smart Scan Server for use with another Trend Micro product (such as OfficeScan), you can use the same server for Threat Mitigator. While Smart Scan Server can be queried simultaneously by multiple Trend Micro products, it may become overloaded as the volume of scan queries increases. Ensure that the Smart Scan Server can handle scan queries coming from different products. Contact your support provider for sizing guidelines and recommendations.

Smart Scan Server Settings

After setting up a Smart Scan Server, specify the server address on the Threat Mitigator console so that endpoints can identify the server to which to send scan queries.

Endpoints send scan queries during On-demand Scan and if a mitigation task uses the Smart Scan Agent Pattern. Network connection is required to connect to this server.

You can also configure endpoints that cannot connect to the Smart Scan Server to send scan queries to the Trend Micro Global Smart Scan Server. Internet connection is required to connect to this server.

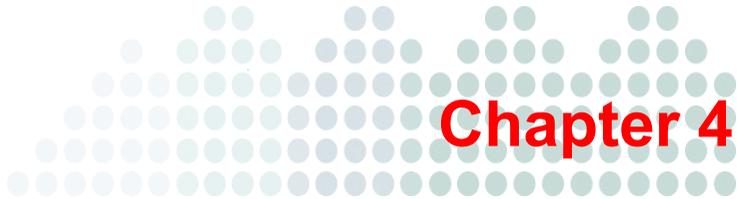
WARNING! The mitigation task or On-demand Scan will not start if connection to both the Smart Scan Server and the Trend Micro Global Smart Scan Server cannot be established.

If the mitigation task or On-demand Scan has started and connection to both servers is lost, files requiring a scan query are bypassed, allowing users to access the file. This event will be logged and logs will be sent to Threat Mitigator. You can view the logs from the threat event logs. For details about threat event logs, see [Threat Event Logs](#) on page 7-2.

To configure Smart Scan Server settings:

PATH: SERVICES > SMART SCAN SERVER

1. Type the Smart Scan Server's address (in URL format). You can find the URL from the Smart Scan Server product console's Summary screen.
2. Select the check box to allow endpoints to connect to the Trend Micro Global Smart Scan Server if connection to the Smart Scan Server cannot be established.
3. Click **Save**.



Deploying Threat Management Agents

This chapter guides you through the Threat Management Agent deployment process and provides instructions on how to manage agent settings from Threat Mitigator.

This chapter includes the following topics:

- *Agent System Requirements* on page 4-2
- *Agent Deployment Methods* on page 4-3
- *Post-installation* on page 4-20
- *Agent Settings* on page 4-21
- *Agent Uninstallation* on page 4-22

Note: To upgrade Threat Management Agents from a previous version, see *Threat Mitigator and Threat Management Agent Upgrades* on page 2-31.

Agent System Requirements

Threat Management Agent requires the following resources:

TABLE 4-1. Threat Management Agent requirements

RESOURCES	REQUIREMENTS
Operating system	<ul style="list-style-type: none">• Microsoft™ Windows™ 2000 (including Professional, Server, and Advanced Server Editions) with Service Pack 4• Windows Server™ 2003 (Standard and Enterprise Editions) with Service Pack 1 or later• Windows XP (Home and Professional Editions) with Service Pack 2 or later• Windows Vista™ (Enterprise, Business, and Ultimate Editions)• Windows Server 2008
Browser	Microsoft™ Internet Explorer™ 6.0 or later if launching the agent installation from the product console

Agent Deployment Methods

Threat Mitigator provides several ways of deploying Threat Management Agent.

TABLE 4-1. Agent deployment methods

DEPLOYMENT METHOD	DESCRIPTION
Using the Packager tool	<p>The Packager tool creates an agent package in Microsoft Installer (MSI) format. After creating the package, you can deploy it to endpoints through Active Directory, Microsoft SMS, or other software deployment applications.</p> <p>For details, see Agent Deployment Using the Packager Tool on page 4-4.</p>
Browser-based installation	<p>Provide users with a link that launches the agent installation program from an Internet Explorer browser window.</p> <p>For details, see Agent Deployment Using Browser-based Installation on page 4-10.</p>
Using TMAgent Manager	<p>TMAgent Manager is a plug-in program available in the Trend Micro OfficeScan server. Use TMAgent Manager to deploy the agent to endpoints managed by the OfficeScan server.</p> <p>For details, see Agent Deployment Using TMAgent Manager on page 4-12.</p>

After installing agents, configure agent settings from the Threat Mitigator console by navigating to **Mitigation Settings > Agent Settings**. Settings apply to all the agents managed by Threat Mitigator. For details about agent settings, see [Agent Settings](#) on page 4-21.

Agent Deployment Using the Packager Tool

Use the Packager tool to create a Microsoft Installer (MSI) package that can be used to install the Threat Management Agent to an endpoint. Launch the tool and create the package on any computer that can access the Threat Mitigator product console.

The tool prompts you to specify the Threat Mitigator IP address so the agent can identify its parent server. It also prompts you for the port number the agent will use to communicate with Threat Mitigator.

To create the agent package:

PATH: MITIGATION SETTINGS > AGENT SETTINGS > AGENT INSTALLATION

1. Click the **Download** link next to **Packager Tool**.
2. Click **Run** twice to launch `TMAgentInstallConfig.exe`.
3. Click **Extract** to copy the files to a temporary folder in the computer. You can also click the button next to the text box to specify a different folder.

The tool's user interface opens.

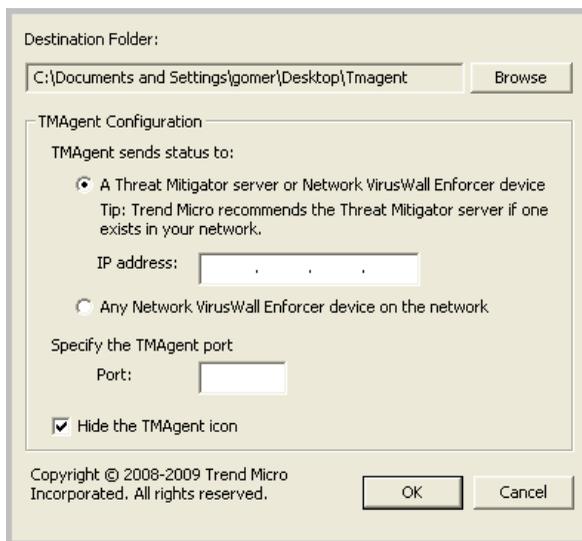


FIGURE 4-1. Packager tool

4. Check the folder to which the agent package will be created. To specify a different folder, click **Browse**.
5. Specify the IP address of the Threat Mitigator server to allow the agent to identify its parent server.
6. Type the agent port number. Ensure that you specify a port number that is currently not in use on target endpoints.
7. (Optional) Choose to hide the agent icon from view. Because Threat Management Agent can be installed silently and does not have settings that users can configure, you may want to enable this option to avoid receiving user inquiries regarding the agent and its functions.
8. Click **OK**. The agent package (`PEAgent.msi`) is created on the folder specified in step 4.

Package Deployment

After creating the agent package, deploy it to endpoints:

- Through Active Directory. For details, see [Package Deployment Using Active Directory](#) on page 4-6.
- Through Microsoft SMS (or other software deployment applications). For details, see [Package Deployment Using Microsoft SMS](#) on page 4-7.
- By creating a logon script that automatically installs the agent on endpoints that log on to a domain. For details, see [Package Deployment Using Logon Script](#) on page 4-9.
- By copying the package to a shared folder accessible to users. For details, see [Package Deployment Using a Shared Folder](#) on page 4-9.
- By launching the package directly on the target computer

Package Deployment Using Active Directory

Take advantage of Active Directory features to deploy the agent package simultaneously to multiple endpoints.

To deploy the package using Active Directory:

1. Open the Active Directory console.
2. Right-click the Organizational Unit (OU) where you want to deploy the package and click **Properties**.
3. On the **Group Policy** tab, click **New**.
4. Choose between **Computer Configuration** and **User Configuration**, and open **Software Settings** below it.

Tip: Trend Micro recommends using **Computer Configuration** instead of **User Configuration** to ensure successful package installation regardless of which user logs on to the computer.

5. Below **Software Settings**, right-click **Software installation**, and then select **New** and **Package**.
6. Locate and select the agent package.
7. Select a deployment method and then click **OK**.
 - **Assigned:** The agent package is automatically deployed the next time a user logs on to the computer (if you selected **User Configuration**) or when the computer restarts (if you selected **Computer Configuration**). This method does not require any user intervention.
 - **Published:** To run the agent package, inform users to go to Control Panel, open the Add/Remove Programs screen, and select the option to add/install programs on the network. When the agent package displays, users can proceed to install the agent.

Package Deployment Using Microsoft SMS

Deploy the agent package using Microsoft System Management Server (SMS) if you have Microsoft BackOffice SMS installed.

The procedure below assumes that the SMS server and agent package are on the same computer. Refer to the Microsoft SMS documentation for other methods of deploying an MSI package.

Known issues when installing with Microsoft SMS:

- "Unknown" appears in the Run Time column of the SMS console.
- If the installation was unsuccessful, the SMS program monitor may still show that the installation has been completed.

The following instructions apply if you use Microsoft SMS 2.0 and 2003.

To obtain the agent package:

1. Open the SMS Administrator console.
2. On the **Tree** tab, click **Packages**.
3. On the **Action** menu, click **New > Package From Definition**. The Welcome screen of the Create Package From Definition Wizard appears.
4. Click **Next**. The Package Definition screen appears.
5. Click **Browse**. The Open screen appears.
6. Browse and select the agent package, and then click **Open**. The agent package name appears on the Package Definition screen. The package shows "Trend Micro Threat Management Agent" and the program version.
7. Click **Next**. The Source Files screen appears.
8. Click **Always obtain files from a source directory**, and then click **Next**. The Source Directory screen appears, displaying the name of the package you want to create and the source directory.
9. Click **Local drive** on site server.
10. Click **Browse** and select the source directory containing the MSI file.
11. Click **Next**. The wizard creates the package. When it completes the process, the name of the package appears on the SMS Administrator console.

To distribute the package to target computers:

1. On the **Tree** tab, click **Advertisements**.
2. On the **Action** menu, click **All Tasks > Distribute Software**. The Welcome screen of the Distribute Software Wizard appears.
3. Click **Next**. The Package screen appears.
4. Click **Distribute an existing package**, and then click the name of the agent package.
5. Click **Next**. The Distribution Points screen appears.
6. Select a distribution point to which you want to copy the package, and then click **Next**. The Advertise a Program screen appears.
7. Click **Yes** to advertise the package, and then click **Next**. The Advertisement Target screen appears.
8. Click **Browse** to select the target computers. The Browse Collection screen appears.
9. Click **All Windows NT Systems**.
10. Click **OK**. The Advertisement Target screen appears again.
11. Click **Next**. The Advertisement Name screen appears.
12. In the text boxes, type a name and your comments for the advertisement, and then click **Next**. The Advertise to Subcollections screen appears.
13. Choose whether to advertise the package to subcollections. Choose to advertise the program only to members of the specified collection or to members of subcollections.
14. Click **Next**. The Advertisement Schedule screen appears.
15. Specify when to advertise the package by typing or selecting the date and time.

If you want Microsoft SMS to stop advertising the package on a specific date, click **Yes. This advertisement should expire**, and then specify the date and time in the **Expiration date and time** list boxes.

16. Click **Next**. The Assign Program screen appears.
17. Click **Yes, assign the program**, and then click **Next**.

Microsoft SMS creates the advertisement and displays it on the SMS Administrator console.

18. When Microsoft SMS distributes the agent package to target computers, a screen displays on each target computer. Instruct users to click **Yes** and follow the instructions provided by the wizard.

Package Deployment Using Logon Script

Create a logon script that installs `PEAgent.msi` when an endpoint joins a domain.

For example:

```
@ECHO OFF
if not exist %windir%\PEAgent\PEAgentMonitor.exe msixexec /i
"\x.x.x.x\PEAgent.msi" /quiet
```

Note: Replace `x.x.x.x` with the IP address of the computer where `PEAgent.msi` is located.

Package Deployment Using a Shared Folder

Copy `PEAgent.msi` to the Web or file server on the Intranet or a shared folder accessible to users.

Agent Deployment Using Browser-based Installation

A link that launches the agent installation program from Threat Mitigator is available on the following product console screens:

- Logon screen



TREND MICRO
Threat Mitigator

Please type your user name and password to access the product console.

User name:

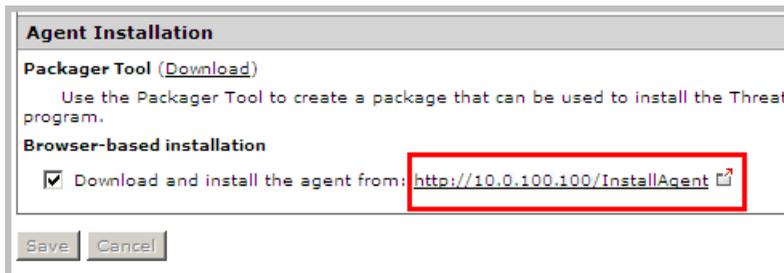
Password:

Threat Management Agent installation:
<http://10.0.100.100/InstallAgent>

On-demand scan:
<http://10.0.100.100/OnDemandScan>

FIGURE 4-2. Agent installation link on the Logon screen

- Agent Settings screen (Mitigation Settings > Agent Settings)



Agent Installation

Packager Tool ([Download](#))

Use the Packager Tool to create a package that can be used to install the Threat program.

Browser-based installation

Download and install the agent from: <http://10.0.100.100/InstallAgent>

FIGURE 4-3. Agent installation link on the Agent Settings screen

To perform browser-based installation:

1. Send the URL to users to allow them to install the agent.
2. Instruct users to perform the following steps:
 - a. Open Internet Explorer and type the URL. The following screen displays.

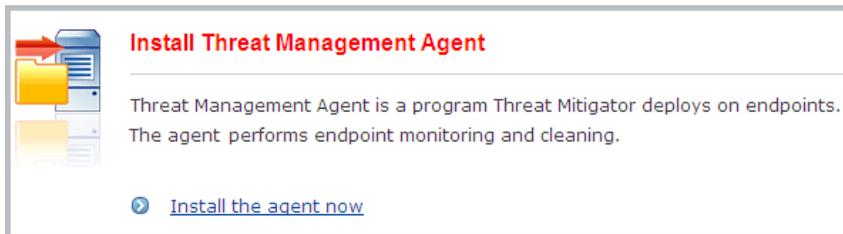


FIGURE 4-4. Browser-based installation screen

- b. Click **Install the agent now** to start the installation. The installation status and result display on the same screen.

Agent Deployment Using TMAgent Manager

This topic discusses how to install TMAgent Manager and deploy Threat Management Agent. For details on managing TMAgent Manager, refer to the Help available from the TMAgent Manager console.

Trend Micro OfficeScan provides a framework (called Plug-in Manager) for deploying security solutions to many endpoints across different platforms. TMAgent Manager is one of the plug-in programs available from Plug-in Manager and is intended for deploying Threat Management Agent to endpoints managed by the OfficeScan server.

Note: TMAgent Manager can only deploy the agent to endpoints managed by the OfficeScan server. If you have several OfficeScan servers, install TMAgent Manager on each server so you can deploy the agent to endpoints managed by these servers.

To deploy the agent to endpoints not managed by any OfficeScan server, use the other agent deployment methods specified in [Agent Deployment Methods](#) on page 4-3.

TMAgent Manager Benefits

TMAgent Manager is useful in the following situations:

- If your network environment does not support automatic deployment of endpoint applications, use TMAgent Manager to find agentless endpoints and then deploy the agent.
- Threat Management Agent can report to both Threat Mitigator and Trend Micro Network VirusWall™ Enforcer. If you have previously set up Network VirusWall Enforcer server, you can configure agents reporting to this server to also report to Threat Mitigator from TMAgent Manager.
- If you have several Threat Mitigator servers, you can configure an agent to report to the other servers from TMAgent Manager.

TMAgent Manager Installation

Like all other OfficeScan plug-in programs, The TMAgent Manager installation package is made available from the OfficeScan server's update source. The default update source is the Trend Micro ActiveUpdate server. However, OfficeScan administrators can set up a custom update source.

When TMAgent Manager is available for download from the update source, it displays on the Plug-in Manager console so you can launch the installation. Plug-in Manager installs TMAgent Manager on the same computer that hosts the OfficeScan server and Plug-in Manager. After the installation, a separate TMAgent Manager console is created and can be accessed from within the OfficeScan server and the Plug-in Manager consoles.

TMAgent Manager Requirements

TMAgent Manager requires the following resources:

- OfficeScan server 8.0 Service Pack 1 or later
- Plug-in Manager 1.0 (apply the latest patch, if available)

Note: For OfficeScan and Plug-in Manager installation requirements and instructions, refer to the documentation for these products.

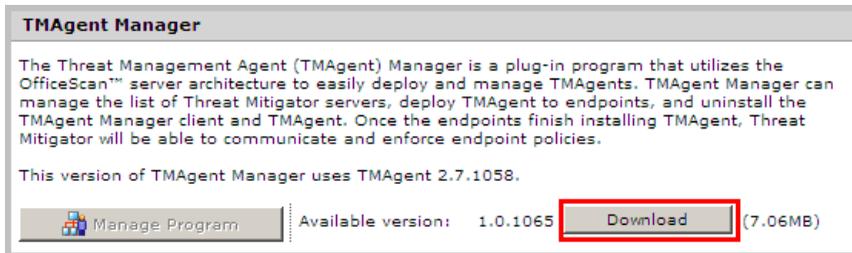
- Check the following if the OfficeScan server obtains updates from a custom update source (and not from the Trend Micro ActiveUpdate server):
 - Ensure that the server computer can connect to the first update source on the list found on the OfficeScan server console's Server Update Source screen (navigate to **Updates > Server > Update Source**). If the server computer cannot connect to the first update source, it does not attempt to connect to the other update sources.
 - Plug-in Manager component list: Check if the first update source contains the latest version of the Plug-in Manager component list (OSCE_AOS_COMP_LIST.xml) and the TMAgent Manager installation package.

To install TMAgent Manager:

1. Log on to the OfficeScan server's Web console and click **Plug-in Manager** on the main menu.

**FIGURE 4-5. OfficeScan Web console main menu**

2. Go to the **TMAgent Manager** section and click **Download**.

**FIGURE 4-6. TMAgent Manager download button**

Note: Plug-in Manager downloads the package to <OfficeScan server installation folder>\PCCSRV\Download\Product.

<OfficeScan server installation folder> is typically
C:\Program Files\Trend Micro\OfficeScan.

3. Monitor the download progress. You can navigate away from the screen during the download.

If you encounter problems downloading the package, check the server update logs on the OfficeScan Web console. On the main menu, click **Logs > Server Update Logs**.

4. After Plug-in Manager downloads the package, a new screen with the following options displays: **Install Now** or **Install Later**.

If you click **Install Now**, agree to the license agreement and then check the installation progress.

If you click **Install Later**:

- a. Open the OfficeScan Web console and click **Plug-in Manager** on the main menu.
- b. Go to the **TMAgent Manager** section and click **Install**.
- c. Agree to the license agreement and then check the installation progress.

After the installation finishes, the Plug-in Manager screen displays the TMAgent Manager version.

5. Verify that TMAgent Manager was installed successfully.
 - The following folder exists: <OfficeScan server installation folder>\Addon\PEAgentManagerServer.

<OfficeScan server installation folder> is typically C:\Program Files\Trend Micro\OfficeScan.
 - The TMAgent Manager registry key exists.
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PEAgentManagerServer

Agent Deployment

From the TMAgent Manager console, add all the Threat Mitigator servers you have set up. When you deploy the agent, you will be prompted to select the Threat Mitigator server to which the agent reports its status.

Note: TMAgent Manager is only used for agent deployment. The agent needs to report to a Threat Mitigator server to run mitigation tasks.

When agent deployment starts, TMAgent Manager sends a command to the endpoint to download and install **TMAgent Manager client**, followed by the Threat Management Agent.

TMAgent Manager client serves as the communication channel between Threat Management Agent and TMAgent Manager. The Threat Management Agent will not be installed if there are problems installing this program. TMAgent Manager client displays on the OfficeScan client's Plug-in Manager screen.

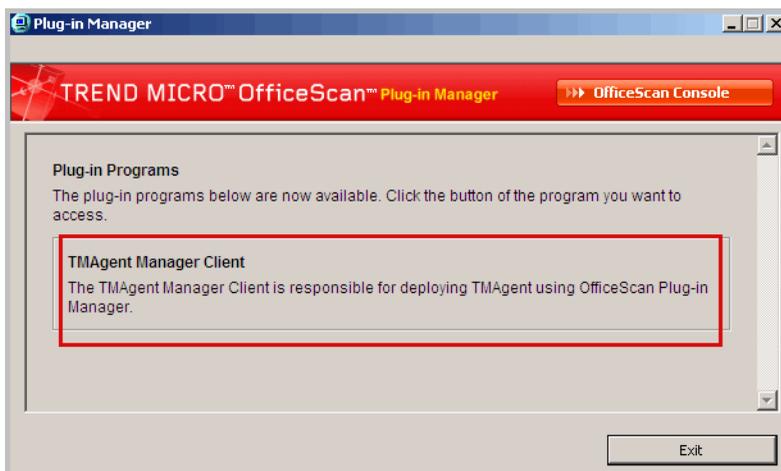


FIGURE 4-7. TMAgent Manager client displayed on the OfficeScan client's Plug-in Manager screen

After TMAgent Manager client installs, Threat Management Agent begins to install. You can check the agent deployment status from the TMAgent Manager console.

When agent deployment is complete, the agent reports its status to its parent Threat Mitigator server. You can query the agent from the Threat Mitigator console. The agent also sends status information to TMAgent Manager.

To deploy the agent from TMAgent Manager:

Part 1: Adding Threat Mitigator to the server list

1. On the **TMAgent Manager** section, click **Manage Program**.



FIGURE 4-8. Manage Program button

2. Click **Manage Server List** from the main menu.



FIGURE 4-9. TMAgent Manager main menu

- Specify Threat Mitigator's IP address, description, and port number in the fields provided.

FIGURE 4-10. Manage Server List screen

- Click **Add Server**. The server name and address appears in the server list.

Part 2: Deploying the agent

- From the client tree on the left section of the screen, select the endpoints to which to deploy the agent.

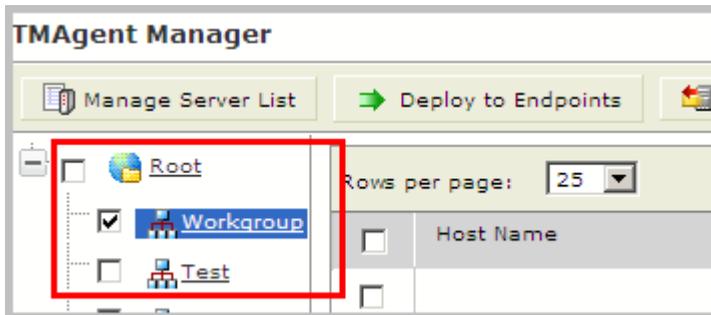


FIGURE 4-11. Client tree

- To select all endpoints belonging to a client tree group, click the check box before the group name.

Note: The group names are identical with the domain names on the OfficeScan server's client tree.

- b. To select specific endpoints, click the group name and then select the endpoints from the endpoint list on the main window.
2. Click **Deploy to Endpoints**. The Deploy to Endpoints screen appears.

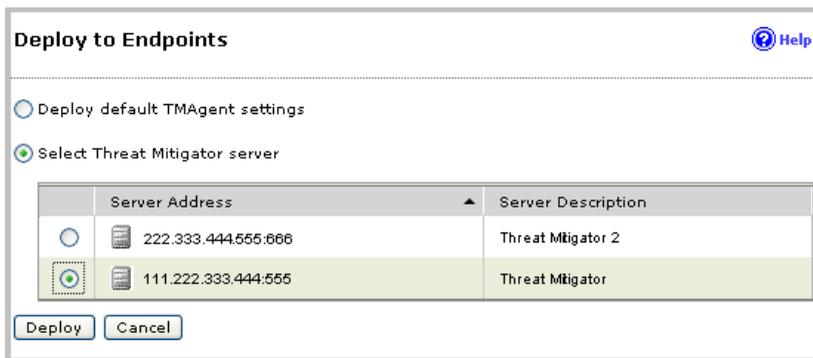


FIGURE 4-12. Deploy to Endpoints screen

3. Select the **Select Threat Mitigator server** option.
4. Select Threat Mitigator from the server list.
5. Click **Deploy**. A confirmation message displays, informing you that agent deployment has started. Refresh the screen after a few minutes to check the deployment result.

Post-installation

Verify the following after deploying agents:

- The agent icon  appears on the endpoint's system tray (if the option to hide the icon was disabled during deployment).
- The agent program exists in %WINDIR%/PEAgent.
- The agent registry key exists.

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Policyenforcer
```
- The agent can be queried from the Threat Mitigator console's Threat Management screen and its status is **Connected**. For details about the tasks you can perform on the Threat Management screen, see [Threat Management](#) on page 5-10.
- If the agent was deployed from TMAgent Manager, the agent version and the Threat Mitigator server to which the agent reports are displayed on the TMAgent Manager console.

Recommended Tasks

Perform the following tasks after deploying agents:

1. Configure global agent settings from the Threat Mitigator console. For details, see [Agent Settings](#) on page 4-21.
2. If you have other Threat Mitigator servers, configure the agent to report to these servers. You can perform this task from the TMAgent Manager console. When an agent loses connection with a particular Threat Mitigator server, another server can issue mitigation tasks to the agent.
3. If Network VirusWall Enforcer is installed, this product can automatically detect and issue policy enforcement tasks to the agent. Policy enforcement ensures that endpoints that connect to the network comply with baseline network security policies. From the TMAgent Manager console's main screen, go to the **Server Address** column and check if the Network VirusWall Enforcer's IP address is listed.

Note: From TMAgent Manager, you can also configure agents already reporting to Network VirusWall Enforcer to also report to Threat Mitigator.

Agent Settings

To ensure proper communication between Threat Mitigator and Threat Management Agent, configure agent settings, which include:

- Port number used by agents to communicate with Threat Mitigator
- Time interval for sending heartbeat messages to Threat Mitigator. A heartbeat message informs Threat Mitigator that a specific agent is up and running and can therefore run mitigation tasks.

Settings apply to all agents managed by Threat Mitigator.

To configure agent settings:

PATH: MITIGATION SETTINGS > AGENT SETTINGS

1. Specify the port number the agent uses to communicate with Threat Mitigator.
2. (Optional) Choose to hide the agent icon on the system tray. Because Threat Management Agent can be installed silently and does not have settings that users can configure, you may want to enable this option to avoid receiving user inquiries regarding the agent and its functions.
3. Under **Agent Status**, specify the time interval for sending heartbeat messages to Threat Mitigator. An agent that is unable to send a heartbeat message at the time interval is considered disconnected.
4. Click **Save**.

Note: The Agent Installation section on the screen allows you to download the packager tool, which you can use to create an MSI package that installs the agent on an endpoint. For details about the tool, see [Agent Deployment Using the Packager Tool](#) on page 4-4.

You can also launch browser-based installation in this section. For details about this agent installation method, see [Agent Deployment Using Browser-based Installation](#) on page 4-10.

Agent Uninstallation

Uninstall the agent if you encounter problems with the agent program and then reinstall it immediately.

When you query agents from Threat Mitigator's Threat Management screen, uninstalled agents may appear in the query result and their status is **Disconnected**. These agents will automatically be removed from the Threat Mitigator database if the agents are not reinstalled within 7 days.

Uninstallation from Control Panel

Like most Windows-based applications, you can uninstall the agent from Control Panel.

To uninstall from Control Panel:

1. Click **Start > Control Panel > Add or Remove Programs**. The Add or Remove Programs screen appears.
2. Locate **Trend Micro Threat Management Agent**, and then click **Remove**. A confirmation dialog box appears.
3. Click **Yes**.

The Threat Management Agent uninstaller checks and removes related settings before removing the files.

Uninstallation from Logon Script

Create a logon script that uninstalls the agent when the endpoint joins a domain.

For example:

```
@ECHO OFF
if exist %windir%\PEAgent\PEAgentMonitor.exe msiexec /uninstall
"\x.x.x.x\PEAgent.msi" /quiet
```

Note: Replace x.x.x.x with the IP address of the computer where PEAgent.msi is located.

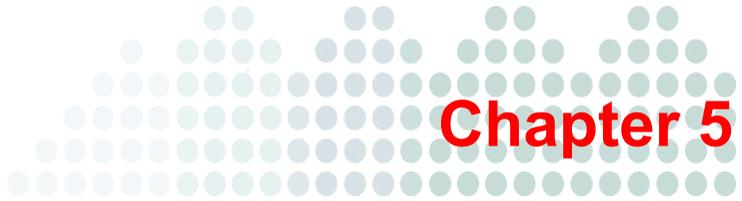
Uninstallation from TMAgent Manager

Agents deployed from TMAgent Manager can be uninstalled remotely from the TMAgent Manager console. The TMAgent Manager client is also removed during uninstallation.

Note: Refer to the TMAgent Manager Help for instructions on uninstalling TMAgent Manager.

To uninstall from TMAgent Manager:

1. Access the TMAgent Manager console.
2. On the client tree, select a group to uninstall all agents belonging to the group. To uninstall specific agents, click the group name and then select the agents from the main window.
3. Click **Uninstall TMAgent**. A confirmation message displays.
4. Check the uninstallation status under the **Status** column.



Performing Threat Mitigation

This chapter discusses how to configure mitigation settings and run mitigation tasks.

Topics in this chapter:

- [Mitigation Settings](#) on page 5-2
- [Mitigation Tasks](#) on page 5-7

Note: For an overview of threat mitigation, see [Threat Mitigation](#) on page 1-4.

Mitigation Settings

Configure the following settings to perform threat mitigation:

1. [Data Sources](#) on page 5-2
 2. [Mitigation Exceptions](#) on page 5-5
 3. [Email Notifications](#) on page 5-6
-

Note: If you have set up Network VirusWall Enforcer, disable the threat mitigation option in Network VirusWall Enforcer policies to avoid feature conflicts. Refer to the Network VirusWall Enforcer documentation for the procedure.

For other guidelines related to Network VirusWall Enforcer installations, see [Network VirusWall Enforcer Installations](#) on page 2-5.

Data Sources

Threat information received from the following data sources prompts Threat Mitigator to issue mitigation tasks to the affected endpoints.

Threat Discovery Appliance

Register Threat Discovery Appliance to Threat Mitigator to allow the appliance to send threat event information. Registration is done from the Threat Discovery Appliance console.

Note: For information on the Threat Discovery Appliance versions compatible with Threat Mitigator, see [Integration with Other Trend Micro Products](#) on page 2-6.

Endpoint Security Risk Logs

Threat Management Agent can monitor Trend Micro™ OfficeScan™ security risk logs and perform mitigation if necessary.

The log monitoring feature supports OfficeScan 10 or later and only checks virus/malware detection logs during Real-time Scan.

Note: OfficeScan provides other scan types, such as Manual Scan and Scheduled Scan.

Threat mitigation is triggered when virus/malware detection logs contain any of the following scan results:

- Quarantined
- Unable to quarantine the file
- Unable to clean or quarantine the file
- Renamed
- Unable to rename the file
- Unable to clean or rename the file
- Deleted
- Unable to delete the file
- Unable to clean or delete the file

During threat mitigation, the agent retrieves the path of an infected file and then uses the Pattern-free Mitigation Engine to check for other files or processes associated with the infected file.

To register Threat Discovery Appliance to Threat Mitigator:

1. Open the Threat Discovery Appliance console.
2. Navigate to **Mitigation > Mitigation Settings**.
3. Click **Enable** beside **Mitigation Device Enforcement**.
4. Type the Threat Mitigator server name or IP address, and description.

5. Specify the IP address ranges that will receive mitigation tasks from Threat Discovery Appliance.

Note: To save network bandwidth, define specific IP addresses for Threat Mitigator. Threat Discovery Appliance only sends mitigation tasks for these specific IP addresses to Threat Mitigator. If the IP address range remains empty, all mitigation requests will be sent to Threat Mitigator.

6. Click **Register**. The Cleanup Settings screen appears.
7. (Optional) Select the **Types of Security Risks/Threats** to send to Threat Mitigator.
8. Click **Apply**.

To configure data sources:

PATH: MITIGATION SETTINGS > DATA SOURCES

1. Select **Monitor virus/malware logs** to allow the agent to monitor security risk logs.

Note: If the option is disabled, the agent stops monitoring security risk logs.

2. Click **Save**.
3. View the Threat Discovery Appliances registered to Threat Mitigator.
4. Use the trash icon  to remove Threat Discovery Appliance from the list.

When you remove the appliance from the list, the appliance continues to send mitigation requests to Threat Mitigator, but Threat Mitigator ignores the requests. Unregister Threat Discovery Appliance from Threat Mitigator to prevent the appliance from sending mitigation requests. Unregistration is done from the Threat Discovery Appliance console.

Mitigation Exceptions

You can exclude IP addresses, process names, or folders from threat mitigation if these items are not vulnerable to threats or are already adequately protected. Add up to 128 mitigation exceptions.

To exclude an endpoint:

PATH: MITIGATION SETTINGS > MITIGATION EXCEPTIONS

1. Type an IP address or IP address range.
2. (Optional) Provide a comment about the IP address. The comment can have a maximum of 150 characters.
3. Click **Add to**. The IP address or IP address range displays in the table.
4. Exclude process or folder names from mitigation actions:
 - a. Select **Enable process and folder exceptions**.
 - b. Specify the **Process or folder name**. You can type up to 255 characters.
 - c. (Optional) Provide a comment about the process or folder name. The comment can have a maximum of 150 characters.
 - d. Click **Add to**. The process or folder name displays in the table.
5. Click **Save**.

Email Notifications

On the product console's Mitigation Tasks screen (which you can access by navigating to **Mitigation Settings > Mitigation Tasks**), you have the option of running threat mitigation tasks automatically or manually. If you choose to manually perform the tasks, configure Threat Mitigator to send you an email informing you of the specific task you need to perform. When you receive the email, access the Threat Management screen to perform the tasks. For details about the tasks you can perform in the Threat Management screen, see [Threat Management](#) on page 5-10.

To configure email notifications:

PATH: ADMINISTRATION > NOTIFICATIONS > EMAIL NOTIFICATIONS

1. Under email settings, type the following:
 - Notification recipient's email address. You can specify several email addresses separated by semi-colons (;).
 - Sender's email address
 - SMTP server name or address
 - SMTP port number
 - SMTP user name
 - SMTP password
2. Click **Send test email** to check if the correct settings were specified and if recipients received the email.
3. Click **Save** if the test email was sent successfully.

Mitigation Tasks

When Threat Mitigator detects that an endpoint requires mitigation, one or several of the following mitigation tasks are carried out:

TABLE 5-1. Mitigation tasks

TASK	DESCRIPTION
Assessment	<p>Threat Mitigator notifies the agent to assess the endpoint after receiving a mitigation request from its data source. During assessment, the agent checks specific objects, processes, and network behavior connected to suspicious activity.</p> <p>The assessment task runs automatically.</p>
Post-assessment cleanup	<p>If the assessment confirms the presence of threats in the endpoint, the agent runs post-assessment cleanup to eliminate threats.</p> <p>You can configure cleanup to run automatically after the assessment or you can run it manually from the Threat Management screen. If you choose to run cleanup manually, enable email notifications. Threat Mitigator sends a notification reminding you to run cleanup. See step 4 below for details about the email notification.</p>
Case submission	<p>When threats are not completely removed from the endpoint after running post-assessment cleanup, a security expert at TrendLabs informs you to submit a case to TrendLabs through Threat Management Services. TrendLabs then issues a custom pattern to eliminate the threats.</p> <p>Case submission is performed from the Threat Management screen and cannot be configured to run automatically.</p>

TABLE 5-1. Mitigation tasks (Continued)

TASK	DESCRIPTION
Custom pattern deployment	<p>Threat Mitigator automatically downloads custom patterns from Threat Management Services. After downloading a pattern, Threat Mitigator deploys it to the affected endpoint and then notifies the agent to run custom cleanup.</p> <p>You can configure custom pattern deployment to run automatically or you can run it manually from the Threat Management screen. If you choose to run pattern deployment manually, enable email notifications. Threat Mitigator sends a notification reminding you to deploy the pattern. See step 4 below for details about the email notification.</p>

To configure mitigation tasks:

PATH: MITIGATION SETTINGS > MITIGATION TASKS

1. Select the tasks that will run when Threat Mitigator detects that an endpoint requires mitigation.
 - **Assess the endpoint only:** Assesses the endpoint based on the information received from data sources. If a threat is found during assessment, run post-assessment cleanup from the Threat Management screen. For details on running post-assessment cleanup, see [Require post- assessment cleanup](#) on page 5-12.
 - **Assess and then automatically run cleanup if required:** Automates the endpoint assessment and post-assessment cleanup tasks. Check the status of the tasks from the threat event logs. For details, see [Threat Event Logs](#) on page 7-2.

If cleanup was unsuccessful, a security expert at TrendLabs notifies you to submit a case. For details in submitting a case, see [Submit a Case to TrendLabs](#) on page 5-18.

2. Specify how to deploy the custom pattern received from TrendLabs.

- **Automatically deploy the pattern and run cleanup:** Automates the custom pattern deployment and custom cleanup tasks. Check the status of the tasks from the threat event logs. For details, see *Threat Event Logs* on page 7-2.
 - **Do not run any task:** Allows you to deploy the custom pattern, which you can perform from the Threat Management screen. After the custom pattern deploys, custom cleanup runs automatically. For details on deploying a custom pattern, see *Require custom cleanup* on page 5-13.
3. Select the scan type to use when the agent runs custom cleanup.
 - **Quick scan:** Scans only the following directories:
 - All fixed drives, such as C:\, D:\, and so on (excludes removable drives)
 - %SystemRoot%
 - %SystemRoot%\system
 - %SystemRoot%\system32
 - %SystemRoot%\system32\drivers
 - %TEMP%
 - **Full scan:** Scans the entire computer
 4. Select **Enable notification** if you chose the following options:
 - **Assess the endpoint only:** Threat Mitigator sends an email after the assessment is complete, notifying you to run post-assessment cleanup.
 - **Do not run any task:** Threat Mitigator sends an email after downloading a custom pattern, notifying you to deploy the pattern to endpoints.

Note: Configure email notification settings from the Email Notifications screen. For details, see *Email Notifications* on page 5-6.

5. Click **Save**.

Threat Management

The Threat Management screen in the product console allows you to run mitigation tasks that are not configured to run automatically. Tasks include:

- Running post-assessment cleanup
- Submitting a case to TrendLabs
- Deploying a custom pattern issued by TrendLabs

The screen also allows you to view endpoints that encountered On-demand Scan problems. If Threat Management Agent exists on the endpoint, you can launch On-demand Scan remotely from the Threat Management screen. For details about launching On-demand Scan remotely, see [To launch On-demand Scan remotely](#): on page 6-12.

Query endpoints by using predefined query criteria or by typing the endpoint's IP address or host name. After the query, you can begin to run threat mitigation tasks and launch On-demand Scan on the affected endpoints.

Predefined Query Criteria

Click the link for each predefined query criteria to display the affected endpoints in the table at the lower section of the screen.

The screenshot displays the Threat Management interface. At the top, the title "Threat Management" is visible. Below it, the "Threat Management: Endpoint Query" section is shown. This section is divided into two columns. The left column, titled "Show endpoints that:", contains three criteria: "Require post-assessment cleanup (0)", "Require custom cleanup (0)", and "Encountered On-demand Scan problems (0)". The right column, titled "Show endpoints that are currently:", contains two options: "Connected (95)" and "Disconnected (449)". Both columns have a red box highlighting the first two items. Below these columns is a "Search endpoint:" field with a search icon and a "Search" button. At the bottom of the interface, there is a table titled "Endpoints Requiring Post-assessment Cleanup". The table has a "Run Cleanup" button and a "Refresh list" button. The table headers are "IP Address", "Host Name", "Current Status", "Status Last Update", and "Connection Status". The table content is currently empty, showing "0-0 of 0" and "Page 0 of 0". The "Endpoints per page" is set to 20.

FIGURE 5-1. Threat Management screen with predefined query criteria highlighted

The following table discusses the tasks you can perform on the endpoints included in the query result.

TABLE 5-2. Predefined query criteria

QUERY CRITERIA	DESCRIPTION	TASKS
Require post-assessment cleanup	Indicates the number of endpoints that require manual cleanup. The number will always be 0 (zero) if you enabled automatic cleanup on the Mitigation Tasks screen (by selecting the option Assess and then automatically run cleanup if required). For details about the Mitigation Tasks screen, see Mitigation Tasks on page 5-7.	<ul style="list-style-type: none">• Click the link to view the affected endpoints in the table at the lower section of the screen.• Select one or more connected endpoints and then click Run Cleanup.• Check the cleanup result from the threat event logs. On the IP Address column, you can click the IP address to open the Threat Event Logs screen.

TABLE 5-2. Predefined query criteria (Continued)

QUERY CRITERIA	DESCRIPTION	TASKS
Require custom cleanup	<p>Indicates the number of endpoints that require manual custom cleanup.</p> <p>When threats are not completely removed from the endpoint after either manual or automatic cleanup, you can submit a case to TrendLabs. TrendLabs then issues a custom pattern to eliminate the threats. After Threat Mitigator downloads the custom pattern, the number in this area is updated to allow you to deploy the pattern and run custom cleanup on the affected endpoint.</p> <p>The number will always be 0 (zero) if you enabled automatic custom cleanup on the Mitigation Tasks screen (by selecting the option Automatically deploy the pattern and run cleanup).</p>	<ul style="list-style-type: none"> • Any of the links below this area indicates the custom pattern needed to run custom cleanup. Click a link to view the affected endpoints in the table at the lower section of the screen. • Select one or more connected endpoints and then click Deploy Pattern. After the pattern deploys, endpoints run custom cleanup. • Check the pattern deployment and custom cleanup results from the threat event logs. On the IP Address column, you can click the IP address to open the Threat Event Logs screen.

TABLE 5-2. Predefined query criteria (Continued)

QUERY CRITERIA	DESCRIPTION	TASKS
Encountered On-demand Scan problems	<p>Indicates the number of endpoints (with or without Threat Management Agent installed) where user-initiated On-demand Scan was launched. The scan was unsuccessful because one or several infected files were not cleaned.</p> <hr/> <p>Note: Unsuccessful On-demand Scans initiated by administrators are not counted in this section. Instead, Threat Management Agent collects endpoint data, which you can then send to TrendLabs through Threat Management Services.</p> <hr/>	<ul style="list-style-type: none"> • Click the link to view the affected endpoints in the table at the lower section of the screen. • For agentless endpoints, instruct users to repeat the scan. • For connected endpoints, select one or more endpoints and then click Launch On-demand Scan to repeat the scan. If this scan encountered issues, Threat Management Agent collects endpoint data to be sent to TrendLabs.

TABLE 5-2. Predefined query criteria (Continued)

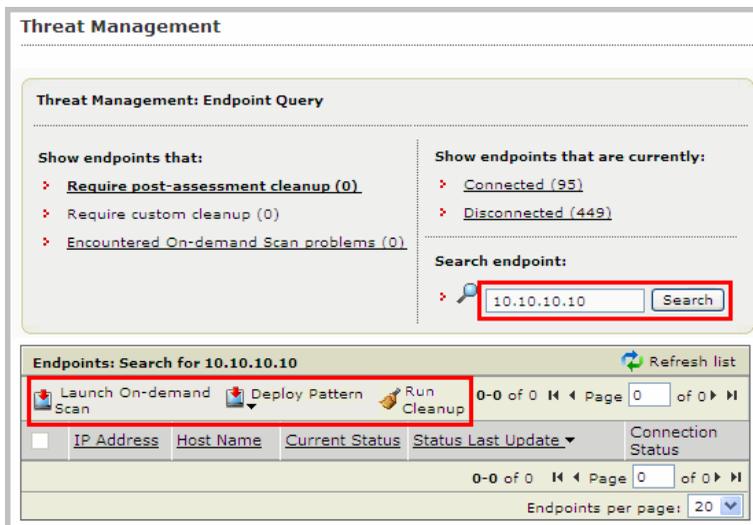
QUERY CRITERIA	DESCRIPTION	TASKS
Connected	<p>Indicates the number of endpoints with Threat Management Agents that can connect to Threat Mitigator. These endpoints may or may not require mitigation.</p> <p>An agent is considered "connected" if it was able to send a heartbeat message to Threat Mitigator at the specified time interval (15 minutes by default). Configure the time interval from the Agent Settings screen. For details, see Agent Settings on page 4-21.</p>	<ul style="list-style-type: none"> Click the link to display the affected endpoints in the table at the lower section of the screen. Check the Current Status column for endpoints that require mitigation or encountered problems executing certain tasks.
Disconnected	<p>Indicates the number of endpoints with Threat Management Agents that cannot connect to Threat Mitigator.</p> <p>An agent is considered "disconnected" if it was unable to send a heartbeat message to Threat Mitigator at the specified time interval.</p> <hr/> <p>Note: The number may also include endpoints with agents reporting to other Threat Mitigator servers, or agentless endpoints that have run On-demand Scan.</p> <hr/>	<ul style="list-style-type: none"> Click the link to display the affected endpoints in the table at the lower section of the screen. Click the icon under Connection Status to run a test connection. The icon turns green if connection was restored.

Endpoints' IP Addresses/Host Names

Type any of the following to display endpoints in the table at the lower section of the screen:

- One or several valid IP addresses. Separate IP addresses by commas.
- A partial IP address (for example, typing 192.168.0 queries all endpoints with IP addresses 192.168.0.1 to 192.168.0.255)
- One or several complete/partial host names. Separate host names by commas.

Note: Endpoints listed in the Mitigation Exceptions screen can be queried but you cannot deploy a custom pattern, run cleanup, or launch On-demand Scan on these endpoints. For details about mitigation exceptions, see [Mitigation Exceptions](#) on page 5-5.



The screenshot displays the Threat Management interface. At the top, it says "Threat Management". Below that is a section titled "Threat Management: Endpoint Query". This section is divided into two columns. The left column, "Show endpoints that:", lists three criteria: "Require post-assessment cleanup (0)", "Require custom cleanup (0)", and "Encountered On-demand Scan problems (0)". The right column, "Show endpoints that are currently:", lists "Connected (95)" and "Disconnected (449)". Below these columns is a "Search endpoint:" field with a magnifying glass icon, containing the text "10.10.10.10" and a "Search" button. A red box highlights this search field. Below the search section is a table header area with the text "Endpoints: Search for 10.10.10.10" and a "Refresh list" button. Below the header are three buttons: "Launch On-demand Scan", "Deploy Pattern", and "Run Cleanup". A red box highlights these three buttons. Below the buttons are several tabs: "IP Address", "Host Name", "Current Status", "Status Last Update", and "Connection Status". At the bottom, there is a pagination bar showing "0-0 of 0" and "Page 0 of 0", and a dropdown menu for "Endpoints per page: 20".

FIGURE 5-2. Threat Management screen with the Search endpoints text box highlighted

When the endpoints display on the table, you can run the following tasks on connected endpoints:

- Launch On-demand Scan. If this scan encountered issues, Threat Management Agent collects endpoint data to be sent to TrendLabs. To send endpoint data, see [Submit a Case to TrendLabs](#) on page 5-18.

Note: For agentless endpoints, provide the On-demand Scan URL to users and instruct them to launch On-demand Scan. For details, see [On-demand Scan on Agentless Endpoints](#) on page 6-7.

- Deploy a custom pattern (recommended on endpoints that require custom cleanup).
- Run cleanup (recommended on endpoints that require post-assessment cleanup).

Submit a Case to TrendLabs

When post-assessment cleanup (manual or automatic) was unable to remove threats completely, Threat Management Agent starts to collect endpoint data. When data collection is complete, a Trend Micro security expert notifies you to send the data to TrendLabs so that a custom pattern can be issued to respond to the threats.

Submit a Case to TrendLabs

Report threat incidents to TrendLabs for further analysis of threat events detected on the following endpoint.

Submit a case to TrendLabs to further analyzing the threat event detected on the following endpoint.

IP Address/Hostname:

Endpoint Details:

IP address: 10.10.10.10

Host Name: HostName

Current status: Data collection completed

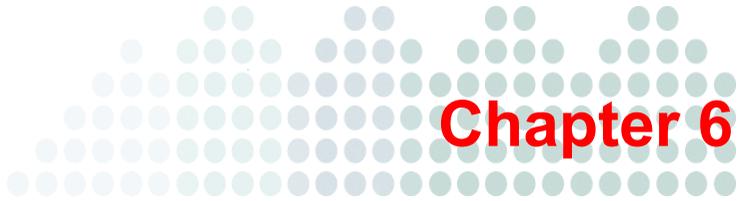
Last status update: 2009/06/30 05:57:59

Connection status: 

FIGURE 5-3. Threat Management screen - Submit a Case to TrendLabs section

To submit a case to TrendLabs:

1. Type the IP address or host name provided by the security expert and click **Search**.
2. Click **Submit**. Threat Management Agent sends the data to Threat Mitigator, which then uploads the data to Threat Management Services. These tasks run automatically and the status for each task is displayed in the **Current Status** field. If there are problems related to these tasks, click **Submit** again.



Performing On-demand Scan

This chapter guides you through the process of setting up and running On-demand Scan on endpoints. For an overview of On-demand Scan, see [On-demand Scan](#) on page 1-6.

This chapter includes the following topics:

- [On-demand Scan Requirements](#) on page 6-2
- [Running On-demand Scan](#) on page 6-7

On-demand Scan Requirements

Prepare or configure the following before running On-demand Scan on endpoints:

- *Smart Scan Server* on page 6-2
- *Endpoint System Requirements* on page 6-3
- *On-demand Scan Settings* on page 6-5
- *Threat Mitigator Components* on page 6-7

Smart Scan Server

On-demand Scan leverages Trend Micro smart scan technology, which requires setting up a Smart Scan Server. Smart scan technology is a next-generation, in-the-cloud based endpoint protection solution. At the core of this solution is an advanced scanning architecture that leverages threat signatures stored in-the-cloud.

For more information about Smart Scan Server, including instructions on setting up the smart scan environment, see *Smart Scan Server Setup* on page 3-17.

Endpoint System Requirements

Before running On-demand Scan, ensure that endpoints meet the following requirements:

System Requirements

On-demand Scan can only be launched on endpoints running 32-bit versions of Microsoft™ Windows™ operating systems.

TABLE 6-1. System requirements for running On-demand Scan

RESOURCES	REQUIREMENTS
Operating system	<ul style="list-style-type: none"> • Windows 2000 with Service Pack 4 • Windows XP with Service Pack 2 or 3 • Windows Server™ 2003 with Service Pack 1 or 2 • Windows Server 2003 R2 with Service Pack 1 or 2 • Windows Vista™ with Service Pack 1 or 2-RTM build • Windows Server 2008 with Service Pack 1 or 2-RTM build
Hardware	<ul style="list-style-type: none"> • Processor: At least 133MHz Intel™ Pentium™ or equivalent • Memory: 64MB minimum • Available disk space: At least 100MB on the system drive (typically drive C:)
Browser	Microsoft Internet Explorer™ 6.0 or later
Others	Monitor that supports 800 x 600 resolution at 256 colors or higher

Network/Internet Connection

Network connection is required to send scan queries to the Smart Scan Server you have installed, and Internet connection to send scan queries to the Trend Micro Global Smart Scan Server.

WARNING! On-demand Scan will not start if connection to both the Smart Scan Server and the Trend Micro Global Smart Scan Server cannot be established.

If On-demand Scan has started and connection to both servers is lost, files requiring a scan query are bypassed, allowing users to access the file. This event will be logged and logs will be sent to Threat Mitigator. You can view the logs from the threat event logs. For details about threat event logs, see [Threat Event Logs](#) on page 7-2.

Additional Disk Space

The On-demand Scan program downloads a set of files to the following location:

<System Drive>/Documents and Settings/<User Name>/Local Settings/Temp/HCEXEC

On-demand Scan files are not removed automatically after each scan session.

With each successive scan, additional disk space on the system drive is used (unless the HCEXEC folder is removed immediately after a scan) for the following reasons:

- Cleaned infected files and other scan-related data (such as detection logs) are added to the HCEXEC folder.
- The On-demand Scan program may download newer versions of components, if available from Threat Mitigator.
- If another user name is used to log on to the computer, a new set of files is downloaded to <System Drive>/Documents and Settings/<Other User Name>/Local Settings/Temp/HCEXEC.

If there is insufficient disk space to run On-demand Scan, consider removing unneeded files in the system drive or emptying the recycle bin. You can also delete the HCEXEC folder. However, performing this task deletes scan-related data obtained from previous On-demand Scans.

On-demand Scan Settings

If Threat Management Agent is not installed on the endpoint, you need instruct users to run On-demand Scan. If the agent is installed, you can run On-demand Scan remotely from the Threat Mitigator console or users can run the scan themselves. For details on running On-demand Scan, see [Running On-demand Scan](#) on page 6-7.

Configure the settings used when you or users run On-demand Scan.

To configure On-demand Scan settings:

PATH: ON-DEMAND SCAN

1. Allow user-initiated scan to run by selecting **Launch the scan from <On-demand Scan URL>**.

Note: The URL can also be found on the Threat Mitigator console's logon page. Clicking the URL launches On-demand Scan.

2. Select the scan type to use during user-initiated scan.
 - **Quick scan:** Scans only the following directories:
 - All fixed drives, such as C:\, D:\, and so on (excludes removable drives)
 - %SystemRoot%
 - %SystemRoot%\system
 - %SystemRoot%\system32
 - %SystemRoot%\system32\drivers
 - %TEMP%
 - **Full scan:** Scans the entire computer
 - **Custom scan:** Scans the folders you have specified

For custom scan, you can specify Windows variables that represent certain system folders. Only the following variables can be specified:

TABLE 6-2. Windows variables

VARIABLE	DESCRIPTION
%ALLUSERSPROFILE%	Returns the location of the All Users Profile
%COMSPEC%	Returns the exact path to the command shell executable
%HOMEDRIVE%	Returns which local workstation drive letter is connected to the user's home directory. Set based on the value of the home directory. The user's home directory is specified in Local Users and Groups.
%SYSTEMDRIVE%	Returns the drive containing the Windows XP root directory (that is, the system root)
%SYSTEMROOT%	Returns the location of the Windows XP root directory
%WINDIR%	Returns the location of the operating system directory
%ALLFIXEDDRIVE%	All fixed drives

3. For administrator-initiated scan, select the scan type.
 - **Quick scan:** Scans only the following directories:
 - All fixed drives, such as C:\, D:\, and so on (excludes removable drives)
 - %SystemRoot%
 - %SystemRoot%\system
 - %SystemRoot%\system32
 - %SystemRoot%\system32\drivers
 - %TEMP%
 - **Full scan:** Scans the entire computer
4. Click **Save**.

Threat Mitigator Components

The On-demand Scan program uses the Smart Scan Agent Pattern and other components available on Threat Mitigator. Ensure that components are up-to-date before running On-demand Scan. For details on updating components, see [Smart Scan Server Setup](#) on page 3-17.

Running On-demand Scan

After setting up the environment required to run On-demand Scan, you or endpoint users can begin to run On-demand Scans.

This topic discusses how to run the scan on agentless endpoints and endpoints with Threat Management Agent installed.

On-demand Scan on Agentless Endpoints

On-demand Scan is intended primarily for agentless endpoints, where routine threat mitigation tasks cannot be performed.

On-demand Scan on agentless endpoints can only be run by endpoint users. You cannot launch the scan remotely from the Threat Mitigator console.

Before asking users to run On-demand Scan:

1. Ensure that the endpoint can connect to Threat Mitigator. The On-demand Scan files are downloaded from Threat Mitigator.
2. Provide users with the On-demand Scan link found on the following Threat Mitigator console screens:

Logon screen



FIGURE 6-1. On-demand Scan link on the Logon screen

On-demand Scan screen

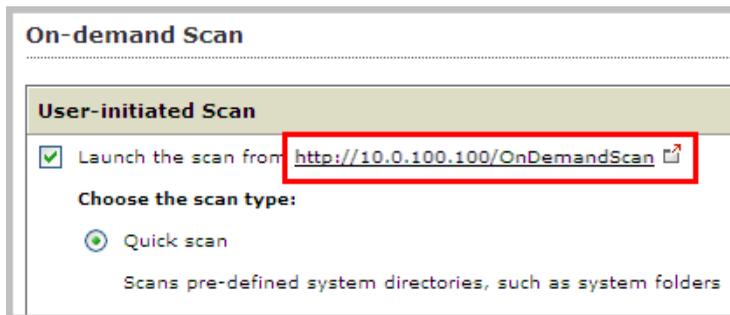


FIGURE 6-2. On-demand Scan link on the On-demand Scan screen

After users launch On-demand Scan, access the Threat Management screen periodically to view endpoints that encountered On-demand Scan problems. Problem details are also available in the threat event logs (see *Threat Event Logs* on page 7-2 for details). You can instruct users to repeat On-demand Scan to resolve the problems.

To run On-demand Scan on agentless endpoints:

Send the following procedure to users who will run On-demand Scan:

1. Type the On-demand Scan URL in an Internet Explorer browser.
2. On the screen that opens, click **Run on-demand scan now**.

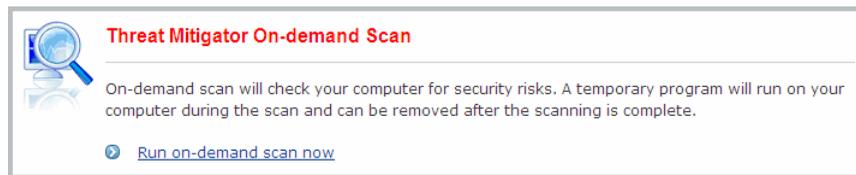


FIGURE 6-3. On-demand Scan start screen

3. A system prompt displays if running the scan for the first time. Click **Install** to continue.

Files begin to download to the endpoint. When all files have been downloaded, a user interface window displays to guide users in launching and completing the scan.

- Accept the terms of the license agreement and then click **Next**.

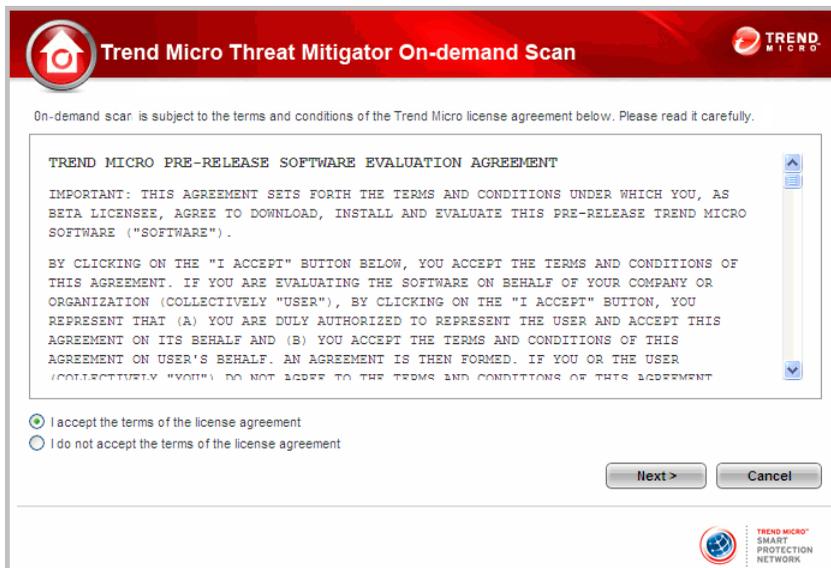


FIGURE 6-4. License agreement screen

- Click **Scan Now**.

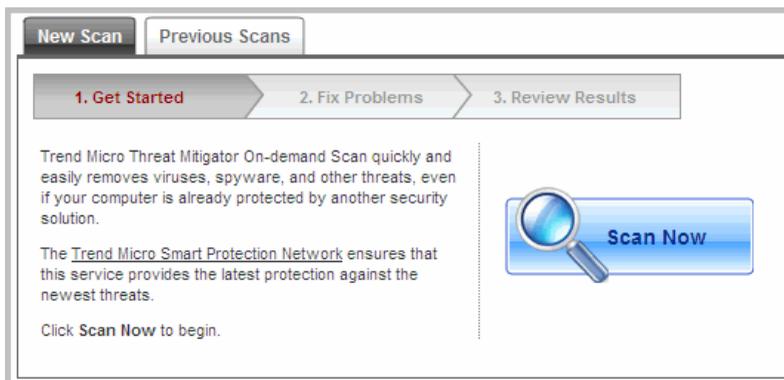


FIGURE 6-5. On-demand Scan main window

The scan progress displays on the same screen.

Note: The number of files to scan depends on the scan type configured from the Threat Mitigator console. For details, see step 2 in the procedure *To configure On-demand Scan settings*: on page 6-5.

6. If threats were found, threat details display on the **2. Fix Problems** tab. If an action was performed under this tab, a summary of the results displays on the next tab **3. Review Results**.
7. Click **Close**.
8. To perform another scan, repeat steps 1 to 6.
9. To view threat details from previous scans, click the **Previous Scan** tab and then select the scan session from the dropdown list.

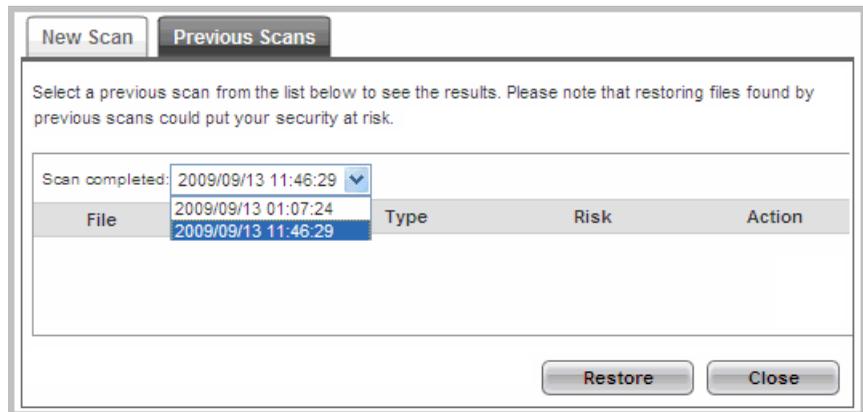


FIGURE 6-6. Previous Scans tab

10. For detected threats that are actually harmless, click **Restore** to move the affected file back to its original location.

On-demand Scan on Endpoints with Agents

On-demand Scan complements routine threat mitigation tasks performed by Threat Management Agent. It allows you to determine an endpoint's overall security posture even if information is not readily available from Threat Mitigator data sources.

You or endpoint users can run On-demand Scan if the agent is installed on the endpoint.

To allow users to run On-demand Scan, see the instructions and guidelines in [On-demand Scan on Agentless Endpoints](#) on page 6-7.

To run On-demand Scan without any user intervention, launch it remotely from the Threat Mitigator console.

Perform the following steps before launching On-demand Scan remotely:

1. Inform the user ahead of time that On-demand Scan will be launched remotely so that the user can prepare the endpoint for the scan. Doing this also ensures that the scan can proceed without problems or delays.
2. Ensure that the Threat Management Agent on the endpoint can connect to Threat Mitigator. You can check the connection status from the Threat Mitigator console.

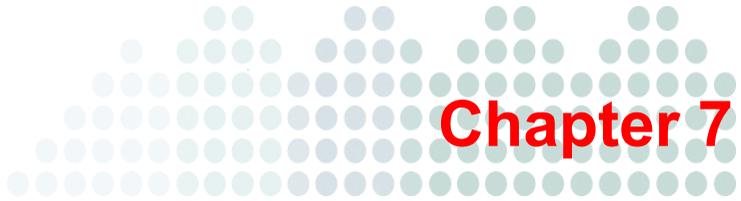
To launch On-demand Scan remotely:

PATH: THREAT MANAGEMENT

1. Type the endpoint's IP address or host name in the **Search endpoint** text box.
2. Verify that the endpoint is connected to Threat Mitigator. On the table on the lower section of the screen, a green-colored icon  displays under the **Connection Status** column.
3. Click **Launch On-demand Scan**.

No user interface displays on the endpoint. All scan tasks (such as downloading of On-demand Scan files and the actual scanning) occur in the background.

If there are issues during scanning, Threat Management Agent collects endpoint data. When a Trend Micro security expert notifies you that endpoint data has been collected, access the Threat Management screen again to submit a case to TrendLabs. For details on submitting a case and other tasks you can perform from the Threat Management screen, see [Threat Management](#) on page 5-10.



Managing Logs

Threat Mitigator keeps comprehensive logs about mitigation events and actions, device events, and endpoint statuses. Use these logs to assess your organization's protection and to identify endpoints with a higher risk of infection.

This chapter contains the following topics:

- *Threat Event Logs* on page 7-2
- *System Logs* on page 7-13
- *Log Transmission to a Syslog Server* on page 7-14
- *Log Maintenance* on page 7-15

Threat Event Logs

Threat Mitigator creates a threat event log entry when performing mitigation actions.

You can do the following from the Threat Event Logs screen:

- View the threat event logs
- Export the logs to a .csv file.
- Perform rollback to restore files, registry keys, and other changes performed by a mitigation action

To query the Threat Event logs:

PATH: LOGS > THREAT EVENT LOGS

1. Select a time period for the query:
 - By default, the **All days** option time period appears in the selection.
 - By default, the date and time of the most recent logs appear in the **To** and **From** fields. Accept the default settings or specify the beginning and ending dates by clicking the calendar icon  next to each field.
2. Click the **More search criteria** link to refine the query scope. Select from the following criteria:

TABLE 7-1. Additional search criteria

SEARCH CRITERIA	DESCRIPTION
IP address or range	The endpoint's IP address
Host name	The endpoint's host name
Threat event	Potential or known threat detections
Data source	The entity that has the capability of reporting threat events to Threat Mitigator, such as Threat Discovery Appliance, endpoint security risk logs (from OfficeScan), Threat Management Services, or the On-demand Scan program launched on an endpoint

TABLE 7-1. Additional search criteria

SEARCH CRITERIA	DESCRIPTION
Mitigation status	<p>Threat events grouped by the following status groups:</p> <ul style="list-style-type: none"> • All: Includes every mitigation status. • Mitigation in progress: The mitigation task is running. • No mitigation: The mitigation task was not performed because of a mitigation exception. • Cleaned threats: All or selected threats have been cleaned. • Scanned endpoint: On-demand Scan has been completed. Either no threat was found or the user chooses to ignore all detected threats. • Assessed endpoint: The agent detected threats in the endpoint during assessment but did not run cleanup because you have chosen to run cleanup manually. • Unsuccessful: The mitigation task was not completed or encountered problems. • Rollback successful: A mitigation task was rolled back successfully. • Rollback unsuccessful: A mitigation task was not rolled back. <hr/> <p>Note: For mitigation status details, see Mitigation Status on page 7-4.</p> <hr/>

3. Click **Search**. A **Query Result** table appears.
4. Click **Rollback** to undo a mitigation task.
5. To export the query results, click **Export to CSV**.

Mitigation Status

This topic discusses the status for the different tasks performed during threat mitigation and On-demand Scan, and the actions to perform when a particular mitigation status displays. The status is recorded in the threat event logs. For details about threat event logs, see *Threat Event Logs* on page 7-2.

Status for Threat Mitigation Tasks

When a threat mitigation task runs, the status of the task is recorded in the Threat Event Logs. For details about threat mitigation tasks, see *Mitigation Tasks* on page 5-7.

TABLE 7-2. Threat mitigation task status

STATUS	DESCRIPTION AND RECOMMENDED ACTIONS
NO ACTION REQUIRED	
Mitigation in progress	Threat Mitigator received an event from a data source and is waiting for the agent to process the mitigation task.
Cleaned threats: All threats cleaned	The agent has cleaned all threats detected on the endpoint.
Rollback successful	The agent successfully rolled back the mitigation action.
ACTION REQUIRED	
Assessed endpoint: Manual cleanup needed	<p>The agent detected threats in the endpoint during assessment but did not run cleanup because you have chosen to run cleanup manually.</p> <p>On the Threat Management screen, click the Require post-assessment cleanup link. On the table at the lower section of the screen, select the endpoint and then click Cleanup.</p>

TABLE 7-2. Threat mitigation task status (Continued)

STATUS	DESCRIPTION AND RECOMMENDED ACTIONS
No mitigation: Mitigation exception	<p>The agent cannot perform the mitigation task because a mitigation exception has been satisfied (for example, if the affected endpoint's IP address is included in the mitigation exception list).</p> <p>Check the threat detected on the endpoint. Consider removing the endpoint from the exception list if you want to run mitigation tasks on the endpoint, and then add the endpoint to the list again after all mitigation tasks have been completed.</p> <hr/> <p>Note: You can also configure mitigation exceptions from Threat Discovery Appliance. While Threat Discovery Appliance scans IP addresses included in its mitigation exclusion list, it does not send mitigation requests to Threat Mitigator if threats are found. Therefore, IP addresses included in the exclusion list of Threat Discovery Appliance are not listed under this status.</p> <hr/>
Unsuccessful: mitigation timeout	<p>The agent did not finish a task within a certain time period. The timeout period for the task cannot be configured.</p> <p>Actions:</p> <ol style="list-style-type: none"> 1. Collect debug logs from endpoints. For details, see Debug Logs on page 9-2. 2. Send the logs to your support provider for analysis.

TABLE 7-2. Threat mitigation task status (Continued)

STATUS	DESCRIPTION AND RECOMMENDED ACTIONS
Unsuccessful: Cannot connect to endpoint	<p>Threat Mitigator notified the agent to run a mitigation task. However, the agent was unreachable for one hour (Threat Mitigator keeps mitigation requests for one hour).</p> <p>Verify the following:</p> <ul style="list-style-type: none"> • The endpoint runs a supported operating system. For details, see Agent System Requirements on page 4-2. • The endpoint successfully installed the agent and the agent is currently running. • The endpoint is up and running, and is able to connect to the network. • There is a functional connection between Threat Mitigator and the agent.
Unsuccessful: Cannot run mitigation task on platform	<p>The agent is running and can run mitigation tasks but the endpoint's operating system does not support the mitigation task.</p> <p>If the endpoint's operating system supports On-demand Scan, try launching the scan from the Threat Management screen or instruct the user to run the scan directly on the endpoint.</p>
Unsuccessful: Incomplete task	<p>Threat Mitigator restarted and was unable to resume pending mitigation tasks.</p> <p>Collect system logs and then send them to your support provider.</p>
Unsuccessful: Not all threats cleaned	<p>The agent was unable to clean all threats.</p> <p>Review the threats listed in the Clean History tab in the Event Details screen. You can manually remove detected threats that you consider harmless.</p>
Unsuccessful: Agent component problem	<p>Files or components used by the agent may be corrupted.</p> <p>Uninstall the agent, restart the endpoint, and then install the agent.</p>

TABLE 7-2. Threat mitigation task status (Continued)

STATUS	DESCRIPTION AND RECOMMENDED ACTIONS
<p>Unsuccessful: Threat no longer exists or requires verification</p>	<p>The agent cannot locate the threat reported by the data source or further investigation is necessary to confirm the presence of the threat.</p> <p>Actions:</p> <ol style="list-style-type: none"> 1. Collect debug logs from endpoints. For details, see Debug Logs on page 9-2. 2. Send the logs to your support provider for analysis.
<p>Unsuccessful: Potential threat requires verification</p>	<p>The agent found potential threats.</p> <p>Actions:</p> <ol style="list-style-type: none"> 1. Collect debug logs from endpoints. For details, see Debug Logs on page 9-2. 2. Send the logs to your support provider for analysis.
<p>Unsuccessful: Agent component error</p>	<p>The agent cannot perform the mitigation task because a component used by the agent encountered an error.</p> <p>Actions:</p> <ol style="list-style-type: none"> 1. Uninstall the agent, restart the endpoint, and then install the agent. 2. If the same error occurs, collect debug logs from the endpoint. For details, see Debug Logs on page 9-2. 3. Send the logs to your support provider for analysis.
<p>Unsuccessful: Corrupted configuration file</p>	<p>A configuration file required to run a mitigation task is corrupted.</p> <p>Actions:</p> <ol style="list-style-type: none"> 1. Collect debug logs from endpoints. For details, see Debug Logs on page 9-2. 2. Send the logs to your support provider for analysis.

TABLE 7-2. Threat mitigation task status (Continued)

STATUS	DESCRIPTION AND RECOMMENDED ACTIONS
Unsuccessful: Pattern not found	<p>A pattern required to run a mitigation task is not available. Run a manual update from the Threat Mitigator console to download the latest patterns.</p> <p>If the missing pattern is a custom pattern issued by TrendLabs, there may be problems between Threat Management Services and Threat Mitigator. Report this problem immediately to your support provider.</p>
Unsuccessful: Cannot connect to Smart Scan Server	<p>The agent cannot start a mitigation task because it cannot connect to the Smart Scan Server or the Trend Micro Global Smart Scan Server.</p> <p>If the agent has started a mitigation task and then loses connection with both scan servers, it bypasses files requiring a scan query. Users can proceed to access the files.</p> <p>Ensure that smart scan settings are correct and that there is a functional connection between the agent and the scan servers. For details, see Smart Scan Server Setup on page 3-17.</p>

TABLE 7-2. Threat mitigation task status (Continued)

STATUS	DESCRIPTION AND RECOMMENDED ACTIONS
Rollback unsuccessful	<p>The agent was unable to completely roll back files, registry keys, or services because the backup file does not exist or is corrupted.</p> <p>To complete the roll back:</p> <ol style="list-style-type: none"> 1. Locate the Task ID for the mitigation task from the Event Details screen. 2. Navigate to <code>C:\%WINDIR%\PEAgent\TDME\backup\F\%TaskID%</code> and check if the backup (.dat) files exist. 3. On the <code>%WINDIR%\PEAgent\TDME</code> folder, type the command <code>TDME.exe /RESTORE %TaskID%</code>. <hr/> <p>Note: Navigate to the Event Details screen of each task to locate TaskID.</p> <hr/> <ol style="list-style-type: none"> 4. If the above steps do not restore files, registry keys, or services, collect debug information from the endpoint. For details, see Debug Logs on page 9-2. 5. Send the log files to your support provider for analysis.

Status for On-demand Scan

When On-demand Scan runs, the status of the scan is recorded in the Threat Event Logs. Users can run On-demand Scan directly on the endpoint. You can also launch it remotely from the Threat Mitigator console. For details about running On-demand Scan, see [Running On-demand Scan](#) on page 6-7.

TABLE 7-3. On-demand Scan status

STATUS	DESCRIPTION AND RECOMMENDED ACTIONS
NO ACTION REQUIRED	
Scanned endpoint: No threat found	<p>On-demand Scan did not find threats on the endpoint.</p> <hr/> <p>Note: The number of files scanned during the scanning session depends on the scan type configured from the Threat Mitigator console. For details about scan types, see To configure On-demand Scan settings: on page 6-5.</p> <hr/>
Cleaned threats: All threats cleaned	On-demand Scan cleaned all the threats detected on the endpoint.
ACTION REQUIRED	
Scanned endpoint: No action performed on threats	<p>Users can manually select the threats to clean during On-demand Scan. During the scan, the user chose to leave all the detected threats uncleaned.</p> <p>Check if there is a reason for not cleaning the threats (for example, if the affected files are required to run the endpoint properly). For threats that you believe are safe to access, send threat samples to your support provider for analysis.</p>

TABLE 7-3. On-demand Scan status

STATUS	DESCRIPTION AND RECOMMENDED ACTIONS
Cleaned threats: All selected threats cleaned	<p>During the scan, all the threats that the user selected for cleaning have been cleaned, but some threats have been left uncleaned.</p> <p>Check if there is a reason for not cleaning the remaining threats (for example, if the affected files are required to run the endpoint properly). For threats that you believe are safe to access, send threat samples to your support provider for analysis.</p>
Unsuccessful: Not all threats cleaned	<p>On-demand Scan was unable to clean some threats possibly because of errors in the On-demand Scan program or the agent (if the agent is installed on the endpoint).</p> <p>Actions:</p> <ol style="list-style-type: none">1. Ask the user to run On-demand Scan again to clean the uncleaned threats.2. If the uncleaned threats cannot be cleaned, collect debug logs from the endpoint. For details, see Debug Logs on page 9-2. Send the logs to your support provider for analysis.

TABLE 7-3. On-demand Scan status

STATUS	DESCRIPTION AND RECOMMENDED ACTIONS
Unsuccessful: Not all selected threats cleaned	<p>During the scan, some of the threats that the user selected for cleaning were not cleaned possibly because of errors in the On-demand Scan program or the agent (if the agent is installed on the endpoint). The user also chose to leave some threats uncleaned.</p> <p>Actions:</p> <ol style="list-style-type: none"> 1. Ask the user to run On-demand Scan again to clean the uncleaned threats. 2. If the uncleaned threats cannot be cleaned, collect debug logs from the endpoint. For details, see Debug Logs on page 9-2. Send the logs to your support provider for analysis. 3. Check if there is a reason for not cleaning the threats the user chose not to clean (for example, if the affected files are required to run the endpoint properly). For threats that you believe are safe to access, send threat samples to your support provider for analysis.
Unsuccessful: Cannot connect to Smart Scan Server	<p>On-demand Scan cannot start because the endpoint cannot connect to the Smart Scan Server or the Trend Micro Global Smart Scan Server.</p> <p>If On-demand Scan is in progress and the endpoint then loses connection with both scan servers, On-demand Scan bypasses files requiring a scan query. Users can proceed to access the files.</p> <p>Ensure that smart scan settings are correct and that there is a functional connection between the endpoint and the scan servers. For details, see Smart Scan Server Setup on page 3-17.</p>

TABLE 7-3. On-demand Scan status

STATUS	DESCRIPTION AND RECOMMENDED ACTIONS
Unsuccessful: Agent component error	On-demand Scan was launched on an endpoint that has an agent installed. A component used by the agent encountered an error. Actions: <ol style="list-style-type: none"> 1. Uninstall the agent, restart the endpoint, and then install the agent. 2. If the same error occurs, collect debug logs from the endpoint. For details, see Debug Logs on page 9-2. 3. Send the logs to your support provider for analysis.

System Logs

Threat Mitigator creates a log entry when the device updates, restarts, or performs other device tasks. Use the System Logs screen to query the system logs.

To query the system logs:

PATH: LOGS > SYSTEM LOGS

1. Select a time period for the query:
 - By default, the **All days** option time period appears in the selection.
 - By default, the date and time of the most recent logs appear in the **From** and **To** fields. Accept the defaults or select beginning and ending dates from the drop down menu or the **From** and **To** fields.
 - Select beginning and end dates from the **From** and **To** fields by clicking the calendar icon  next to each field and the individual date. The date you clicked appears in the respective **From** or **To** field in the correct format.
2. Click the **More search criteria** link. Additional detailed input fields appear.

3. Refine your search by selecting any combination of the following:
 - Severity
 - Event
 - Description
4. Select the number of logs per page that you wish to display.
5. Click **Search**. A **Query Result** table appears.

Note: To export your query results to a `.csv` file, click the **Export to CSV** link.

Log Transmission to a Syslog Server

Threat Mitigator supports sending logs to syslog servers.

To configure the syslog server settings:

PATH: LOGS > SYSLOG SERVER SETTINGS

1. Select the check box to send logs to the primary syslog server.
2. Type the IP address and port number of the primary syslog server.
3. (Optional) Select the check box to send logs to the secondary syslog server to manage logs on a backup or duplicate syslog application.
4. Type the IP address and port number of the secondary syslog server.
5. Click **Save**.

Log Maintenance

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or enable automatic log deletion.

To automatically delete logs:

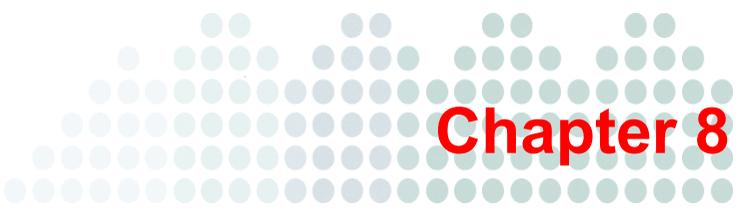
PATH: LOGS > MAINTENANCE

1. Click the **Automatic** tab.
2. Select the check box to enable automatic deletion of logs.
3. Specify the type of logs to delete. You can delete system logs and threat event logs.
4. Specify the number of days to keep the logs. Logs older than the number of days are automatically deleted. The default value is 30 days.
5. Click **Save**.

To manually delete logs:

PATH: LOGS > MAINTENANCE

1. Click the **Manual** tab.
2. Specify the type of logs to delete. You can delete system logs and threat event logs.
3. Choose whether to delete all logs for the selected log types or only logs older than a certain number of days. The default value is 30 days.
4. Click **Delete Now**.



Chapter 8

Performing Administrative Tasks

To ensure that Threat Mitigator continues to work properly, perform the administrative and maintenance tasks described in this chapter.

This chapter includes the following topics:

- *HTTPS Certificate* on page 8-2
- *Administrative Accounts* on page 8-3
- *Access Control* on page 8-4
- *SNMP Settings* on page 8-5
- *IP Address Settings* on page 8-8
- *Static Route Settings* on page 8-9
- *Configuration Backup and Restore* on page 8-10
- *Threat Mitigator Restart* on page 8-11
- *Support Tools* on page 8-12
- *Appliance Firmware Flash Utility* on page 8-13

HTTPS Certificate

View the Threat Mitigator HTTPS certificate and replace the certificate if you have obtained a more recent version.

Use the following command to generate a certificate from a Linux operating system:

```
openssl req -new -x509 -days 365 -nodes -out FILE_NAME.pem -keyout  
FILE_NAME.pem
```

To manage the HTTPS certificate:

PATH: ADMINISTRATION > DEVICE CONFIGURATION > HTTPS CERTIFICATE

1. View certificate details.
2. If you have obtained a more recent certificate, click **Replace Certificate**.
3. On the screen that appears, browse to the location of the certificate and then click **Import Certificate**.

Administrative Accounts

Use administrative accounts to grant users access to the product and preconfiguration consoles. If there are several Threat Mitigator administrators in your organization, this feature helps you delegate administrative tasks to the administrators. In addition, you can grant non-administrators "view" access to the product console.

To add an administrative account:

PATH: ADMINISTRATION > ADMINISTRATIVE ACCOUNTS

1. Click **Add**.
2. Type the user ID and password for the account, and then confirm the password.
3. Select the privileges for the account.
 - **Administrator:** Has complete access to the product and preconfiguration consoles.
 - **Power User:** Can manage the product and preconfiguration consoles, but cannot create administrative accounts.
 - **Operator:** Can view configuration information from the product console, but cannot log on to the preconfiguration console.
4. Click **Save**.
5. Send the administrative account details to the users.

Access Control

Configure Access Control settings to regulate access to the Threat Mitigator console.

To configure Access Control settings:

PATH: ADMINISTRATION > DEVICE CONFIGURATION > ACCESS CONTROL

1. For a more secure access to the product console, enable access using the SSH protocol.

Note: To change the SSH console access from the preconfiguration console, connect to Threat Mitigator using a direct console connection.

2. To prevent certain IP addresses from accessing the console, select **Enable IP address restriction**. You can add up to 20 IP addresses to this list.
 - a. Type an IP address in the IP address text box.
 - b. (Optional) Type a comment. For example, specify a reason for adding the IP address to the list.
 - c. Click **Add to**.
3. Select **Enable Custom Message** and then type the message that users will see when console access is denied.
4. Click **Save**.

SNMP Settings

Simple Network Management Protocol (SNMP) is a set of protocols used in managing network devices, such as bridges, routers, and hubs over a TCP/IP network.

In the SNMP management architecture, one or more computers on the network act as a network management station (NMS) and poll the managed devices to gather information about their performance and status. Each managed device has a software module, known as an agent, which communicates with the NMS.

Security

Managed devices can protect their Management Information Base (MIBs) by granting only specific network management stations access. One way of doing this is through authentication. Managed devices can require that all NMSs belong to a community, the name of which acts as a password that the managed devices use to authenticate management stations attempting to gain access. Additionally, the settings for a community can include access privileges, such as READ-ONLY and READ-WRITE, that are granted to NMSs.

Table 8-1 and *Table 8-2* enumerate the supported Threat Mitigator SNMP specifications:

TABLE 8-1. Supported SNMP Agent specifications

SPECIFICATIONS	COMMUNITY-BASED SNMPv2 (SNMPv2c)
Access privileges	READ ONLY (the GET command)
Management Information Base (MIB)	MIB II, with the following standard objects: <ul style="list-style-type: none"> • System group • Interfaces group • Enterprise group, including system status and memory utilization

TABLE 8-1. Supported SNMP Agent specifications (Continued)

SPECIFICATIONS	COMMUNITY-BASED SNMPv2 (SNMPv2c)
Accepted community names	Community names with the following characteristics: <ul style="list-style-type: none"> • Default name: public • Access privileges: READ ONLY (the get command) • Maximum number of community names: 5 • Maximum length of community name: 33 alphanumeric characters
Trusted Network Management Stations (NMS)	Allows up to 255 specific network management station IP addresses to access the agent

SNMP Agent Limitations

The following are the SNMP agent limitations:

- Version supported: 2c
- **Community Names:** One community name allowed
- **Community name character limitation:** 1–33 alphanumeric characters (including underscore: "_")
- **Destination NMS IP addresses:** One NMS IP address allowed per community name
- **System location and System contact:** 0–254 characters (ASCII 32–126, excluding "&")

SNMP Traps

In addition to the standard SNMP traps, Threat Mitigator defines the following additional traps:

TABLE 8-2. Supported SNMP Traps specifications

SPECIFICATIONS	DETAILS
Community name	One community name allowed
Destination Network Management Station (NMS) IP addresses	One NMS IP address allowed per community name

TABLE 8-3. SNMP Traps

SNMP TRAP	DESCRIPTION
Cold start	Enable SNMP
Shutdown	Shut down Threat Mitigator
Boot to factory default	Boot to default rescue partition. An SNMP trap is sent every minute.
Boot to previous partition	Boot to the previous partition by typing. This sends an SNMP trap after booting to the previous partition.

To configure SNMP settings:

PATH: ADMINISTRATION > NOTIFICATIONS > SNMP SETTINGS

1. Select the check box to enable SNMP Trap.
2. Type the **Community name** and **Server IP address**.
3. Select the check box to Enable SNMP Agent.
4. Type the **System location** and **System contact**.
5. Type a **Community name** to add under **Accepted Community Name(s)**. You can add up to 5 SNMP Accepted Community Names.
6. Click **Add to**. The community name displays in the table.

7. Type the IP Address to add under **Trusted Network Management IP Address(es)**. You can add up to 255 SNMP Trusted Network Management IP Addresses.
8. Click **Add to**. The IP address displays in the table.
9. Click **Save**.
10. To export the MIB file:
 - a. Click **Export MIB file**.
 - b. Save the file to the preferred location on the computer.

IP Address Settings

You can change the Threat Mitigator IP address from the product console. However, changing the IP address will cause agents to lose connection with Threat Mitigator. Before changing the IP address, contact your support provider first for instructions on how agents can maintain connection with Threat Mitigator even if the IP address changes.

Note: You can also configure IP address settings from the preconfiguration console. For details, see [Phase 3: Configuring the IP Address](#) on page 2-27.

Threat Mitigator, Smart Scan Server, and the VMware ESX/ESXi server (which hosts the Smart Scan Server and Threat Mitigator) require unique IP addresses. Check the IP addresses of the VMware ESX/ESXi server and Smart Scan Scan Server and ensure that none of these IP addresses is assigned to Threat Mitigator.

If you have set up Network VirusWall Enforcer, add the Threat Mitigator IP address to the Global Endpoint Exception List in Network VirusWall Enforcer. Refer to the Network VirusWall Enforcer documentation for the procedure.

Note: For other guidelines related to Network VirusWall Enforcer installations, see [Network VirusWall Enforcer Installations](#) on page 2-5.

To configure the IP address settings:

PATH: ADMINISTRATION > NETWORK CONFIGURATION > IP ADDRESS SETTINGS

1. Specify the following:
 - Host name
 - IP address
 - Subnet mask
 - Default gateway
 - Primary DNS server
 - Secondary DNS server
2. If there is a separate management network in your environment, select to enable a separate management interface, and then type the IP address and subnet mark of the management interface.
3. Click **Save**.

Static Route Settings

Configure static route settings to route data directly between Threat Mitigator and network segments.

To configure the static routes settings:

PATH: ADMINISTRATION > NETWORK CONFIGURATION > STATIC ROUTES

1. Click **Add**.
2. Under **Static Route Settings**, type the **Network ID**, **Subnet Mask**, and **Router**.
3. Click **Save**.

Configuration Backup and Restore

Back up the Threat Mitigator configurations and settings by exporting them to a file. You can then import the file to restore settings in case of a problem. You can also use the file to import configurations and settings to other Threat Mitigator servers.

Note: Threat Mitigator needs to restart after importing the configurations.

To manage configurations:

PATH: ADMINISTRATION > BACKUP CONFIGURATION

1. To export configurations to a file:
 - a. Click **Backup**.
 - b. Save the file to the preferred location on the computer.
2. To import configurations from a file:
 - a. Click **Browse**.
 - b. Locate and then select the file to import.
 - c. Click **Open**.

WARNING! Ensure that you back up the current configurations before proceeding so you can restore the configurations if there are problems with the imported file.

3. Click **Import Configuration**. Threat Mitigator restarts after importing the configuration settings.

Threat Mitigator Restart

The following events require Threat Mitigator to restart:

- Importing a configuration file from the preconfiguration console or product console
- Automatically or manually updating the Threat Mitigator program file (if the program version requires a restart) from the product console

Restart Threat Mitigator from the product from the product console or from the preconfiguration console.

WARNING! Ensure that all tasks have been completed before restarting Threat Mitigator. If there are uncompleted tasks, the "Action Unsuccessful: Device restarted" message appears.

To restart Threat Mitigator from the product console:

PATH: ADMINISTRATION > SYSTEM MAINTENANCE

1. Click **Restart Now**.
2. Confirm the restart when prompted.

Support Tools

Use the following Threat Mitigator tools to help you perform administrative tasks and obtain information that can be used to troubleshoot product issues.

On the product console, navigate to **Administration > Support Tools** to download and use these tools.

TABLE 8-4. Support tools available for download

TOOL	DESCRIPTION
System Information Collector (SIC) Tool	SIC gathers detailed computer configuration that helps isolate and identify known or potential threats in an endpoint.
Case Diagnostic Information	Case Diagnostic Information downloads information required for use with the Case Diagnostic Tool. The tool is used for debug purposes.
Sysclean Tool	<p>The Trend Micro SysClean Tool is a stand-alone fix package that incorporates the Trend Micro malware and spyware scanning engines, as well as the Trend Micro Damage Cleanup Engine and Template.</p> <p>The SysClean Tool:</p> <ul style="list-style-type: none"> • Terminates detected malware/spyware instances in memory • Removes malware/spyware registry entries • Remove malware/spyware entries from system files • Scans for and deletes detected malware/spyware copies
System Log Viewer	System log viewer runs in the syslog server to receive and display system logs.
Program Rescue Tool	The program rescue tool is used for restoring the default Threat Mitigator images.

Appliance Firmware Flash Utility

Threat Mitigator provides the Appliance Firmware Flash Utility to update the Threat Mitigator program file. The utility is a graphical user interface tool that provides a user-friendly method of uploading the most recent program file. The utility is included in the *Trend Micro Solutions CD for Threat Mitigator*.

Entering Rescue Mode

If you encounter problems with Threat Mitigator, enter rescue mode to upload the program file. When in rescue mode, Threat Mitigator uses the default static IP address. See [Table 8-5](#) for a summary of rescue mode settings.

TABLE 8-5. Rescue mode settings

RESCUE MODE SETTING	VALUE
Threat Mitigator host name	Blank
IP address type	Reset
IP address	192.168.252.1
Subnet Mask:	255.255.255.0
Default gateway	192.168.252.254
DNS server 1	Blank
DNS server 2	Blank

Note: Appliance Firmware Flash Utility stops and will not be able to function if you do not configure these settings. Use the Windows **Task Manager** utility if the utility becomes non-responsive.

To enter rescue mode through the preconfiguration console:

1. Log on to the Threat Mitigator preconfiguration console.
2. Select **Restart Device** from **System Tasks**.
3. When the device restarts, a message appears prompting you to enter rescue mode.
4. Type `r` at the prompt. The Threat Mitigator rescue mode settings appear.

Uploading the Program File

The Threat Mitigator program file (firmware) contains all the components necessary to prepare Threat Mitigator for preconfiguration. The program file includes the operating system, virus scan engine, pattern file, and system programs.

Note: Uploading the program file restores the Threat Mitigator default factory settings.

To preserve the existing settings, back up the Threat Mitigator configuration from the **Administration > Backup Configuration** screen. After uploading the new or default program file, re-configure the device settings from the preconfiguration console's **Device Settings** menu or import the original configuration from the **Administration > Backup Configuration** screen.

Note: After the new firmware is deployed to Threat Mitigator, the device automatically restarts.

The program file name is as follows:

```
SDK_image.STD_PAE-VMWARE-BUSYBOX.x.yy.zzzz.en_US.R
```

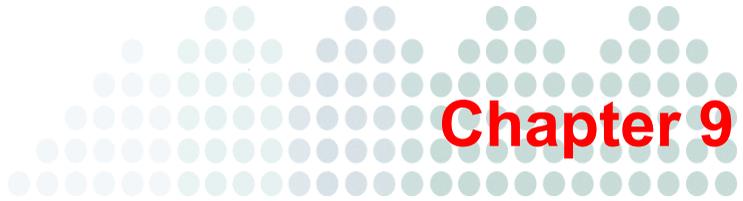
Where:

- x is the major version
- yy is the minor version
- zzzz is the build number
- en_US is the program language version
- R denotes the nature of the file (that is, the Threat Mitigator program file)

You can obtain the program files from the following locations:

- **Trend Micro download Web site:** Contains the most recent versions
<http://www.trendmicro.com/download>
- **Trend Micro Solutions CD for Trend Micro Threat Mitigator:** The included CD contains the program file with factory defaults and the original boot loader. These files are located in the following path (replace D: with the path used by your CD-ROM drive):

```
D:\Programs\TM_Rescue\
```

Troubleshooting and Support

This chapter provides basic troubleshooting tasks and discusses how to contact Trend Micro.

This chapter contains the following topics:

- *Debug Information* on page 9-2
- *Troubleshooting* on page 9-4
- *Contacting Trend Micro* on page 9-7

Debug Information

To analyze and troubleshoot product issues, collect debug information and send the debug logs to your support provider. You can also include error messages or system prompts that display when you encountered the issues.

Endpoint Debug Information

Collect the following information from the endpoints.

Endpoint Information

To collect endpoint information, use the System Information Collector (SIC) tool available for download from the product console's **Administration > Support Tools** screen.

Registry Keys

Export the Threat Management Agent registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Policyenforcer
```

Debug Logs

Collect the following log files:

Note: %WINDIR% indicates the Windows directory, for example, C:\Windows.

- All the files in the %WINDIR%\PEAgent folder
- Threat Management Agent deployment debug log
 - %WINDIR%\PEAgentDeployLog.txt
 - %temp%\PEAgentDeployLog.txt
- Threat Management Agent main debug logs:
 - %WINDIR%\PEAgent\PEAgentLog.txt
 - %WINDIR%\PEAgent\PEAgentLog.txt.bak
- Threat Management Agent system tray icon debug log:
 - %WINDIR%\PEAgent\PEAgentMonitor.txt
- Threat Management Agent upgrade debug log:

- %WINDIR%\PEAgent\msilog.txt
- %temp%\PEAConfig.txt or PEAconfig.txt.bak
- Vulnerability Assessment debug log:
 - %WINDIR%\PEAgent\tmva\Debug*.*
- Threat mitigation debug logs:
 - %WINDIR%\PEAgent\TDME\TDMEAgentDebugLog.log
 - %WINDIR%\PEAgent\TDME\Debug*.*
 - %WINDIR%\PEAgent\TDME\report*.*
 - %WINDIR%\PEAgent\TDME\TDMEEventLog*.*

Threat Mitigator Debug Information

Collect the debug logs using the Case Diagnostic Tool. For details, see [Case Diagnostic Information](#) on page 8-12.

Troubleshooting

Some problems may have causes that are not readily apparent. Before contacting technical support, identify the problem by investigating the following possible causes:

Device Settings and Configuration

Unable to read packets

Problem: The network card drops packets after verification.

Solution: Ensure that the Threat Mitigator Data Interface is assigned to the VMware ESX virtual switch, and that the virtual switch is assigned to a physical network adapter.

Unable to Unregister Threat Discovery Appliance from Threat Mitigator

Problem: The administrator unregistered Threat Discovery Appliance from Threat Mitigator using the trash bin icon. However, the Threat Discovery Appliance still displays Threat Mitigator as a registered device.

Solution: Unregister Threat Mitigator from the Threat Discovery Appliance product console.

Endpoint Settings

Unable to display endpoint notification screen

Problem: The Threat Mitigator endpoint notification screen does not display if the Threat Mitigator device and Network VirusWall Enforcer device are on the same network.

Solution: Add the Threat Mitigator IP address to the Network VirusWall Global Endpoint Exception list.

Scan Failure Due to Data Execution Prevention (DEP)

Problem: Threat Mitigator sometimes fails to clean a client machine if the client machine has enabled Data Execution Prevention (DEP)

Note: DEP is a Windows feature available only in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows Server 2003 with Service Pack 1.

Solution 1: Add the Threat Mitigator client agent, `RMAgent.exe` in the `%windir%\PEAgent\TDME` folder into the DEP exception list. To get to the DEP exception list, follow the procedure below.

To add `RMAgent.exe` to the DEP exception list:

1. While logged on to the client computer as Administrator:
 - a. Click **Start > Run**.
 - b. Type the following: `sysdm.cpl`
 - c. Click **OK**.The System properties multi-tabbed window appears.
2. On the **Advanced** tab, under Performance, click **Settings**. The Performance Options window appears.
3. Click the **Data Execution Prevention** tab and select the **Turn on DEP for all programs and services except those I select**: radio button. The **Add...** button below activates.
4. Click **Add...** A file manager window appears.
5. Navigate to the location of the `RMAgent.exe` file on the client machine and click that file name. A box with a green check appears next to the name `RMAgent.exe` in the field above the **Add...** button.
6. Click **OK** twice.

Solution 2: Download Microsoft Application Compatibility Toolkit and apply its compatibility fix, DisableNX, to Threat Mitigator client agent `RMAgent.exe`. Save the fix as an `.sdb` file and deploy the fix to the specific endpoints by one of the following methods:

- **Email attachment:** The custom database can be sent through email to the users who require the fixes. If users are running Windows XP, they can simply choose to run the attachment.
- **Floppy disk:** The "Sneaker Net" approach. Copy the database file onto removable media and use that media to install the database on multiple endpoints. (Best suited to a small number of endpoints in close walking distance.)
- **Network folder:** Endpoints can manually install the compatibility database from a shared network location.
- **Push install:** You can include the custom database in an installation package that you deploy through push technology. Possible solutions include Microsoft Systems Management Server (SMS) or Group Policy within Active Directory domains.
- **Logon script:** Does not require user interaction and can be custom-tailored for different groups of users based on the logon script that they receive.

As an example of how a logon script might be used, consider the following:

```
if not exist %systemroot%\appatch\RMAgentFix.sdb sdbinst.exe -q  
\\server1\compat\RMAgentFix.sdb
```

Excluding Endpoints From Mitigation Tasks

Problem: Some endpoints can be excluded from mitigation events.

Solution: Add the endpoint IP address to the Mitigation Exclusion List from the Threat Discovery Appliance product console.

Contacting Trend Micro

This section discusses how to contact Trend Micro, access Trend Micro online resources, and provide documentation feedback.

Technical Support

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

Trend Micro Incorporated provides worldwide support to all registered users.

- Visit the following URL:

http://us.trendmicro.com/us/about/contact_us/

Click the link for the required region. Follow the instructions for contacting support in your region.

- Get the latest Trend Micro product documentation at:

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

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

Trend Micro, Inc.

10101 North De Anza Blvd., Cupertino, CA 95014

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

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

Fax: +1 (408) 257-2003

Web address:

<http://www.trendmicro.com>

Email: support@trendmicro.com

Speeding Up Your Support Call

To speed up your problem resolution, run Case Diagnostic Information (see *Case Diagnostic Information* on page 8-12 for details) or ensure that you have the following details available:

- Operating system
- Network type
- Brand and model of the computer and connected hardware
- Amount of memory and free hard disk space on your machine
- Detailed description of the installation environment
- Exact text of any error message
- Steps to reproduce the problem

The Trend Micro Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro Web site, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

<http://esupport.trendmicro.com>

Trend Micro updates the contents of the Knowledge Base continuously and adds new solutions daily. If you are unable to find an answer, however, you can describe the problem in an email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

Security Information Center

Comprehensive security information is available at the Trend Micro Web site.

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

Information available:

- List of viruses and malicious mobile code currently "in the wild," or active
- Computer virus hoaxes
- Internet threat advisories
- Virus weekly report
- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Glossary of terms

TrendLabs

TrendLabsSM is the global antivirus research and support center of Trend Micro. Located on three continents, TrendLabs has a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

You can rely on the following post-sales service:

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

TrendLabs has achieved ISO 9002 quality assurance certification.

Sending Suspicious Files to Trend Micro

If you think you have an infected file but the scan engine does not detect it or cannot clean it, Trend Micro encourages you to send the suspect file to us. For more information, refer to the following site:

<http://subwiz.trendmicro.com/subwiz>

You can also send Trend Micro the URL of any Web site you suspect of being a phish site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and viruses).

- Send an email to the following address and specify "Phish or Disease Vector" as the subject.

virusresponse@trendmicro.com

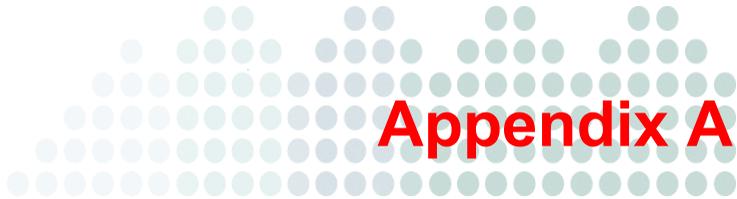
- You can also use the Web-based submission form at:

<http://subwiz.trendmicro.com/subwiz>

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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



Glossary

Additional Threats

Files and programs, other than viruses, that can negatively affect the performance of the computers on your network.

Agentless Endpoints

Endpoints that do not have Threat Management Agent installed. On the Threat Management screen, a red-colored icon under the **Connection Status** column indicates either an agentless endpoint, or an endpoint that has Threat Management Agent installed but cannot connect to Threat Mitigator.

Connected Endpoints

Endpoints that have Threat Management Agent installed. The agents can connect to Threat Mitigator and can therefore run mitigation tasks. On the Threat Management screen, a green-colored icon appears under the **Connection Status** column to indicate that the agent is connected.

Dynamic Host Control Protocol (DHCP)

A device, such as a computer or switch, must have an IP address to be connected to a network, but the address does not have to be static. A DHCP server, using the Dynamic Host Control Protocol, can assign and manage IP addresses dynamically every time a device connects to a network.

Dynamic IP Address (DIP)

A Dynamic IP address is an IP address that is assigned by a DHCP server. The MAC address of a computer will remain the same, however, the computer may be assigned a new IP address by the DHCP server depending on availability.

File Transfer Protocol (FTP)

FTP is a standard protocol used for transporting files from a server to a client over the Internet. Refer to Network Working Group RFC 959 for more information.

Hypertext Transfer Protocol (HTTP)

HTTP is a standard protocol used for transporting Web pages (including graphics and multimedia content) from a server to a client over the Internet.

HTTPS

Hypertext Transfer Protocol using Secure Socket Layer (SSL).

Internet Control Message Protocol (ICMP)

Occasionally a gateway or destination host uses ICMP to communicate with a source host, for example, to report an error in datagram processing. ICMP uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and must be implemented by every IP module. ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. The Internet Protocol is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable.

Internet Protocol (IP)

"The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)

Malware

Malware refers to any program that executes and performs activities that are outside of the user's consent. A virus is a form of malware. Other examples of malware include Trojans, Worms, Backdoors, Denial of Service attacker agents, Joke programs, as well as several other smaller categories of malicious code.

Ping

A utility that sends an Internet Control Message Protocol (ICMP) echo request to an IP address and waits for a response. The Ping utility can determine whether or not the machine with the specified IP address is online or not.

Secure Socket Layer (SSL)

SSL is a scheme proposed by Netscape Communications Corporation to use RSA public-key cryptography to encrypt and authenticate content transferred on higher level protocols such as HTTP and FTP.

Telnet

Telnet is a standard method of interfacing terminal devices over TCP by creating a "Network Virtual Terminal". Refer to Network Working Group RFC 854 for more information.

Test Virus

An inert file that acts like a real virus and is detectable by virus-scanning software. Use test viruses, such as the EICAR test script, to verify that your antivirus installation is scanning properly.

Transmission Control Protocol (TCP)

A connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multi-network applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for information.

TrendLabs

TrendLabs is Trend Micro's global network of antivirus research and product support centers that provide 24 x 7 coverage to Trend Micro customers around the world.

Virus

A virus is a program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes.

Index

A

- access control 8-4
- Activation Code 3-7
- Active Directory 4-6
- ActiveUpdate server 3-13
- administrator account 8-3
- agent package 4-4
- agentless endpoint 1-6, 6-7, 6-9
- Anti-rootkit Driver 3-11
- Antivirus Product Detection Engine 3-11
- Appliance Firmware Flash Utility 8-13
- assessment 5-7

B

- backup 8-10, 8-14
- browser-based installation 4-3, 4-10

C

- capacity test 2-3
- Case Diagnostic Information 8-12
- case submission 5-10, 5-13, 5-18
- certificate 8-2
- cleanup
 - custom 1-5, 5-8, 5-13
 - post-assessment 5-7, 5-12
- component updates 3-10, 6-7
- components 3-10, 6-7
- configurations 8-10–8-11
- custom pattern 1-5, 5-8, 5-13
- custom scan 6-5

D

- Damage Cleanup Engine 3-11
- Damage Cleanup Template 3-11
- data source 1-4, 5-2
- debug information 9-2
 - Threat Management Agent 9-2
 - Threat Mitigator 9-3
- DEP 9-5
- deployment
 - custom pattern 5-8, 5-13
 - Threat Management Agent 4-3
- documentation feedback 9-10

E

- endpoint assessment 1-4
- endpoint query 5-11, 5-16
- exceptions 5-5

F

- features and benefits 1-8
 - new features 1-2
- fresh installation 2-7
- full scan 5-9, 6-5

H

- heartbeat message
 - Threat Management Agent 4-21
 - Threat Mitigator 3-8
- HTTPS certificate 8-2

I

- installation
 - Threat Management Agent 1-8, 4-3

- Threat Mitigator 2-7
- TMAgent Manager 4-13–4-14
- IP address 2-27, 8-8

K

- Knowledge Base 3-3, 9-8

L

- license 3-7
- logon
 - account 8-3
 - product console 3-2
- logon script 4-9, 4-22
- logs
 - maintenance 7-15
 - OfficeScan 5-3
 - On-demand Scan 7-10
 - send to Syslog server 7-14
 - system logs 7-13
 - threat events 7-2
 - Threat Mitigator 7-1

M

- management network 2-2, 2-16, 2-24, 2-29, 8-9
- manual update 3-14
- Microsoft SMS 4-7
- mitigation exceptions 5-5
- mitigation task
 - assessment 1-4
 - custom cleanup 5-8, 5-13
 - custom pattern deployment 1-5, 5-8
 - endpoint assessment 5-7
 - manual 5-10
 - post-assessment cleanup 5-7, 5-12
 - rollback 1-8, 7-3–7-4
- MSI package 4-4

N

- network adapter 2-14, 2-22
- Network Management Station (NMS) 8-6
- Network VirusWall Enforcer 4-12, 4-20
- notifications
 - email 5-6, 5-9
 - SNMP 8-5
- NTP server 3-7

O

- OfficeScan
 - Plug-in Manager 4-12
 - security risk logs 5-3
- On-demand Scan 1-6
 - on agentless endpoints 6-7
 - on endpoints with agents 6-12
 - remote scan 6-12
 - scan types 6-5
 - settings 6-5
 - status 7-10
 - system requirements 6-3
 - troubleshooting 5-10, 5-14, 6-9, 6-12
- operator account 8-3
- OVF file 2-10–2-11, 2-18

P

- Packager tool 4-3–4-4
- password 3-6
- Pattern-free Mitigation Engine 3-10
- Pattern-free Mitigation Template 3-10
- Plug-in Manager 4-12
- post-assessment cleanup 5-7, 5-12
- post-installation 4-20
- power user account 8-3
- preconfiguration console 2-27
- product configurations 8-10

- product console 3-2
 - access control 8-4
 - banner 3-3
 - logon 3-2, 8-3
 - main content window 3-5
 - main menu bar 3-4
 - password 3-6
- program file 8-14
- program rescue tool 8-12
- promiscuous mode 2-17
- proxy server authentication 3-16
- proxy settings 3-16

Q

- quick scan 5-9, 6-5

R

- registration
 - Threat Discovery Appliance 5-3
 - Threat Management Services 3-9
- rescue mode 8-13
- restart 8-11
- RMAgent 9-5
- rollback 1-8, 7-3–7-4

S

- scan query 1-4, 6-4
- scheduled updates 3-15
- smart scan 1-8, 6-2
- Smart Scan Agent Pattern 3-10
- Smart Scan Server 3-10, 6-2, 6-4
- SNMP 8-5
- static routes 8-9
- suspicious files 9-10
- Sysclean tool 8-12
- syslog server 7-14

- System Clean and Forensic Module 3-10
- System Information Collector (SIC) 8-12
- System log viewer 8-12
- system logs 7-13
- system requirements
 - On-demand Scan 6-3
 - Threat Management Agent 4-2
 - Threat Mitigator 2-2
 - TMAgent Manager 4-13
- system time 3-7

T

- technical support 9-7
- Threat Discovery Appliance 5-2
 - register Threat Mitigator to 5-3
 - unregister Threat Mitigator from 2-33
- threat event logs 7-2
- Threat Management Agent 1-4, 3-11
 - connection status 5-15
 - deployment 1-8
 - deployment methods 4-3
 - post-installation 4-20
 - settings 4-21
 - system requirements 4-2
 - uninstallation 2-33, 4-22
- Threat Management Services 3-8, 3-16
- threat mitigation 1-4, 1-8
 - data source 5-2
 - endpoint query 5-11
 - exceptions 5-5
 - status 7-4
 - tasks 1-4, 5-7, 5-17
- Threat Mitigator
 - about 1-4
 - backing up 8-10
 - capacity 2-3

- components 3-10, 6-7
- data source 1-4
- features and benefits 1-8
- fresh installation 2-7
- getting started 3-1
- HTTPS certificate 8-2
- installation package 2-10
- integration with Trend Micro products and services 1-6
- IP address 2-27, 8-8
- license and Activation Code 3-7
- logs 7-1
- powering on 2-17, 2-25
- product console 3-2
- program file 8-14
- proxy settings 3-16
- rescue mode 8-13
- restart 8-11
- server list 4-17
- support tools 8-12
- system requirements 2-2
- uninstallation 2-33
- TMAgent Manager 4-3, 4-12
- TMAgent Manager client 4-16
- tools 8-12–8-13
- Trend Micro Global Smart Scan Server 3-18, 6-4
- Trend Micro Solutions CD 8-15
- TrendLabs 5-10, 5-13, 5-18, 9-9
- troubleshooting
 - general 9-4
 - mitigation tasks 7-4
 - On-demand Scan 7-10

U

- uninstallation
 - Threat Management Agent 2-33, 4-22

- Threat Mitigator 2-33
- unregistration 2-33
- update source
 - Threat Mitigator 3-13
- updates 3-10, 6-7
 - manual 3-14
 - methods 3-14
 - scheduled 3-15
- URL
 - agent installation 4-10
 - On-demand Scan 6-5, 6-8
 - product console 3-2
 - Smart Scan Server 3-18

V

- virtual machine 2-2
- virtualization 2-2
- Virus Scan Engine 3-10
- VMware ESX/ESXi server 2-7, 3-17
- VMware Infrastructure Client 2-8, 2-18
- vSphere Client 2-8, 2-11

W

- what's new 1-2