TREND MICRO™

Threat Mitigator 2.6

Administrator's Guide

TREND MICRO™ SMART PROTECTION NETWORK™

Endpoint Security

Network Security

Protected Cloud

Document Part No. APEM24567/100810

Release Date: October 2010

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 website.

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

Chapter 1: Introducing Threat Mitigator

Chapter 2: Installation, Upgrade, and Uninstallation

Chapter 3: Getting Started

Chapter 4: Deploying Threat Management Agents

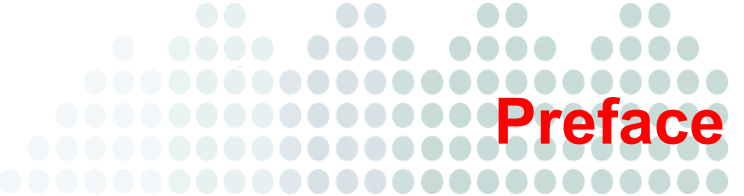
Chapter 5: Performing Threat Mitigation

Chapter 6: Running On-demand Scan

Chapter 7: Viewing and Analyzing Information

Chapter 8: Performing Administrative Tasks

Chapter 9: Troubleshooting and Support



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

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 website: 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
Italics	References to other documentation or new technology components
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.

TABLE P-2. Document conventions (Continued)

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

Chapter 1

Introducing Threat Mitigator

This chapter introduces Threat Mitigator features and capabilities.

This chapter includes the following topics:

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
Control Manager integration	Threat Mitigator integrates with Trend Micro Control Manager starting in this release. For integration details, see *Trend Micro Control Manager* on page 3-24.
Post-installation scan	Scan an endpoint for threats immediately after installing the agent. For details, see *Agent Settings* on page 3-22.
Endpoint status	Monitor the security status of endpoints from the Endpoint Status screen. For details, see *Endpoint Status* on page 7-2.
Threat management enhancement	In the Threat Management screen, you can now perform the following tasks: • View endpoints that require a restart • Launch On-demand Scan on several or all connected endpoints For details, see *Threat Management* on page 5-10.
Custom pattern enhancement	• Custom patterns no longer expire. • By default, Threat Mitigator keeps 5 custom patterns in its storage directory.

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 works with Threat Management Agent installed on each endpoint to provide the following protection types:

- Threat Mitigation
- On-demand Scan

> **Note:** On-demand Scan can also be run on an endpoint without Threat Management Agent.

Threat Mitigator is part of Threat Management Services, a threat lifecycle management suite that brings together security experts and a host of solutions to provide ongoing security services. For details, see *About Threat Management Services* on page 1-12.

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
- Post-assessment Cleanup
- Threat Analysis
- Pattern Deployment and Custom Cleanup

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 protection 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 protection source. For details about smart protection sources, see *Smart Protection Technology* on page 3-18.

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.

Threat Analysis

Threat Management Agent collects forensic data with information about unresolved threats and sends the data to Threat Mitigator. Threat Mitigator then uploads the data to **Threat Management Services Portal (TMSP)**.

TMSP monitors endpoints that require further mitigation. It is available as a Trend Micro **hosted service** and as an **on-premise application** that you can install on a bare metal server or a virtual machine.

If you have TMSP as a hosted service, a Trend Micro security expert will inform you about the unresolved threats, and will ask you to submit a case so that the threat can be analyzed. After the analysis, Trend Micro provides a pattern file to address the threat.

If you have TMSP as an on-premise application, perform case submission from the Threat Management screen and then log on to TMSP's administrative console for information on unresolved threats. You can then send the information to Trend Micro for analysis and wait for the pattern file.

Pattern Deployment and Custom Cleanup

Run custom cleanup to eliminate unresolved threats. Any of the patterns listed in *Table 1-2* can be used during custom cleanup.

TABLE 1-2. Pattern files that can be used during custom cleanup

PATTERN TYPE	DESCRIPTION
Custom pattern	Trend Micro creates a custom pattern in response to a particular threat. Custom patterns are deployed through TMSP. If you have TMSP as a hosted service, a security expert at Trend Micro uploads the pattern to TMSP. If you have TMSP as an on-premise application, obtain the pattern from Trend Micro and then upload it to TMSP. The availability of custom patterns depends on your service agreement with Trend Micro. Contact your Trend Micro representative for details about your service agreement. Threat Mitigator keeps 5 custom patterns by default.
Smart protection patterns	If custom patterns are not available to you, newer versions of smart protection patterns (either **Smart Scan Agent Pattern** or **Smart Scan Pattern**, or **both**) may be able to eliminate unresolved threats. Smart protection patterns are regularly updated to respond to the latest threats and are released through the Trend Micro ActiveUpdate server. These patterns are continuously available for download as long as the product license is valid. Information about specific pattern versions that can be used to run custom cleanup can be obtained from Trend Micro.

When a custom pattern or smart protection patterns become available, the following process is initiated:

TABLE 1-3. Pattern deployment and custom cleanup process

	IF USING A CUSTOM PATTERN	IF USING SMART PROTECTION PATTERNS
1	Threat Mitigator automatically downloads the custom pattern from TMSP.	If scheduled updates is enabled, Threat Mitigator updates the Smart Scan Agent Pattern, while the Smart Protection Server updates the Smart Scan Pattern. **Note:** Manually update the patterns if scheduled updates is disabled.
2	If automatic pattern deployment is enabled, Threat Mitigator deploys the custom pattern/Smart Scan Agent Pattern to a particular endpoint. If disabled, manually deploy the pattern from the Threat Management screen. When you click the **Require custom cleanup** link on the screen, the pattern version displays. **Note:** You can enable or disable automatic pattern deployment from the Mitigation Tasks screen.	
3	Threat Mitigator notifies Threat Management Agent to run custom cleanup using the custom pattern/Smart Scan Agent Pattern. **Note:** If the Smart Scan Agent Pattern cannot verify the risk of the file, the agent queries the Smart Scan Pattern.	
4	The agent reports the cleanup results 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 protection technology used during threat mitigation.

Integration with Trend Micro Products and Services

Threat Mitigator integrates with the following Trend Micro products and services. For seamless integration, ensure that the products run the required or recommended versions.

TABLE 1-4. Products and services that integrate with Threat Mitigator

PRODUCT	DESCRIPTION	VERSION
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. **Note:** Threat Discovery Appliance is part of Threat Management Services. For details, see *About Threat Management Services* on page 1-12.	• 2.6 (recommended) • 2.5R2 • 2.55 • 2.0 (minimum)
Threat Management Services Portal (TMSP)	A security portal used for collecting forensic data from specific endpoints and issuing custom solutions to eliminate unresolved threats. **Note:** TMSP is part of Threat Management Services. For details, see *About Threat Management Services* on page 1-12.	2.6 (for the on-premise edition of TMSP)

TABLE 1-4. Products and services that integrate with Threat Mitigator (Continued)

PRODUCT	DESCRIPTION	VERSION
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.	10.0 (minimum)
Smart Protection Network™	Provides the file reputation service, an in-the-cloud hosted solution that verifies potential threats detected during post-assessment cleanup or On-demand Scan. Endpoints connected to the corporate network send scan queries to Smart Protection Network if a Smart Protection Server is unavailable to confirm the risk of a file. Smart Protection Network is hosted by Trend Micro. For details, see *Smart Protection Technology* on page 3-18.	Not applicable
Smart Protection Server	Provides the same file reputation service offered by Smart Protection Network. Smart Protection Server is intended to localize the service to the corporate network to optimize efficiency. Endpoints connected to the corporate network send scan queries to Smart Protection Server if the risk of a file cannot be confirmed.	• 2.0 (recommended) • 1.1 Service Pack 1 • 1.0 (minimum)

TABLE 1-4. Products and services that integrate with Threat Mitigator (Continued)

PRODUCT	DESCRIPTION	VERSION
Control Manager	A software management solution that gives you the ability to control antivirus and content security programs from a central location—regardless of the platform or the physical location of the program. For details, see *Trend Micro Control Manager* on page 3-24.	5.5

Key Features and Benefits

Threat Mitigator provides the following features and benefits:

TABLE 1-5. 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.
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.
Agentless protection	With On-demand Scan, you can extend 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 protection technology	Trend Micro smart protection 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 4-2.

About Threat Management Services

Today's workplace is changing as new and emerging technologies enable people to work with increased mobility. This shift has brought about a new type of threat, one that can enter a network through these technologies and is sophisticated enough to evade detection by existing security infrastructure. For example, threats are unknowingly introduced into the network by employees and guests who bring with them infected mobile computers and portable storage devices. Technologies such as peer-to-peer applications, streaming media, instant messaging, and other potential infection channels can be easily exploited by hackers and cyber criminals, especially if usage is unregulated.

Organizations without dedicated security personnel and with lenient security policies are increasingly exposed to threats, even if they have basic security infrastructure in place. Once discovered, these threats may have already spread to many computing resources, taking considerable time and effort to eliminate completely. Unforeseen costs related to threat elimination can also be staggering.

Trend Micro Threat Management Services provides organizations with an effective way to discover, mitigate, and manage stealthy and zero-day internal threats. Threat Management Services brings together security experts and a host of solutions to provide ongoing security services. These services ensure timely and efficient responses to threats, identify security gaps that leave the network vulnerable to threats, help minimize data loss, significantly reduce damage containment costs, and simplify the maintenance of network security.

Threat Management Services combines years of Trend Micro network security intelligence and in-the-cloud servers that are part of Trend Micro's Smart Protection Network to identify and respond to next-generation threats.

The following diagrams illustrate how Threat Management Services work:

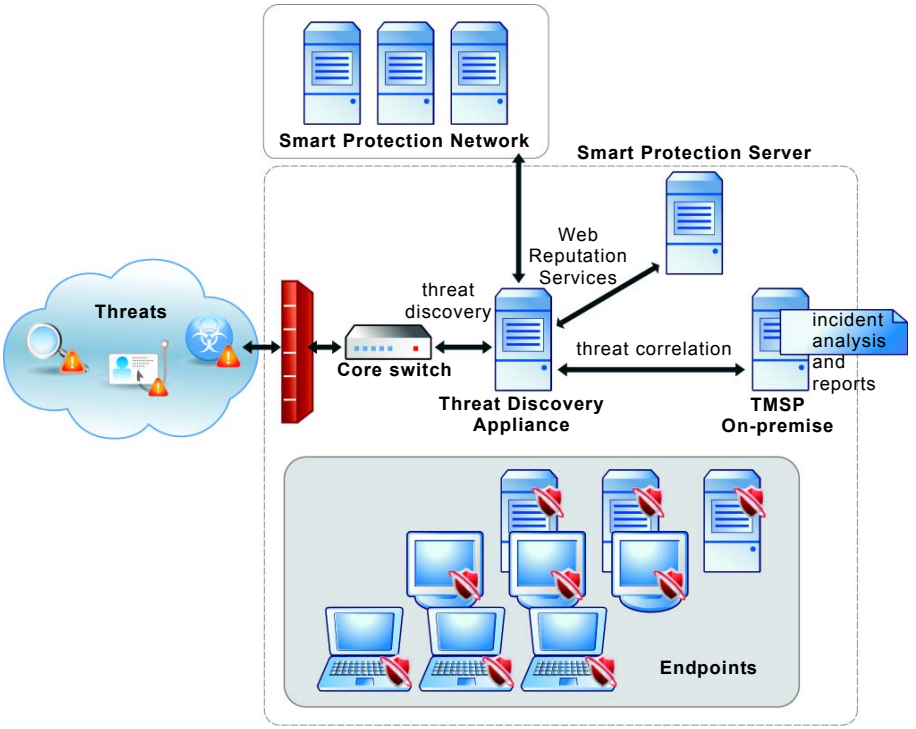


FIGURE 1-1. Threat discovery process

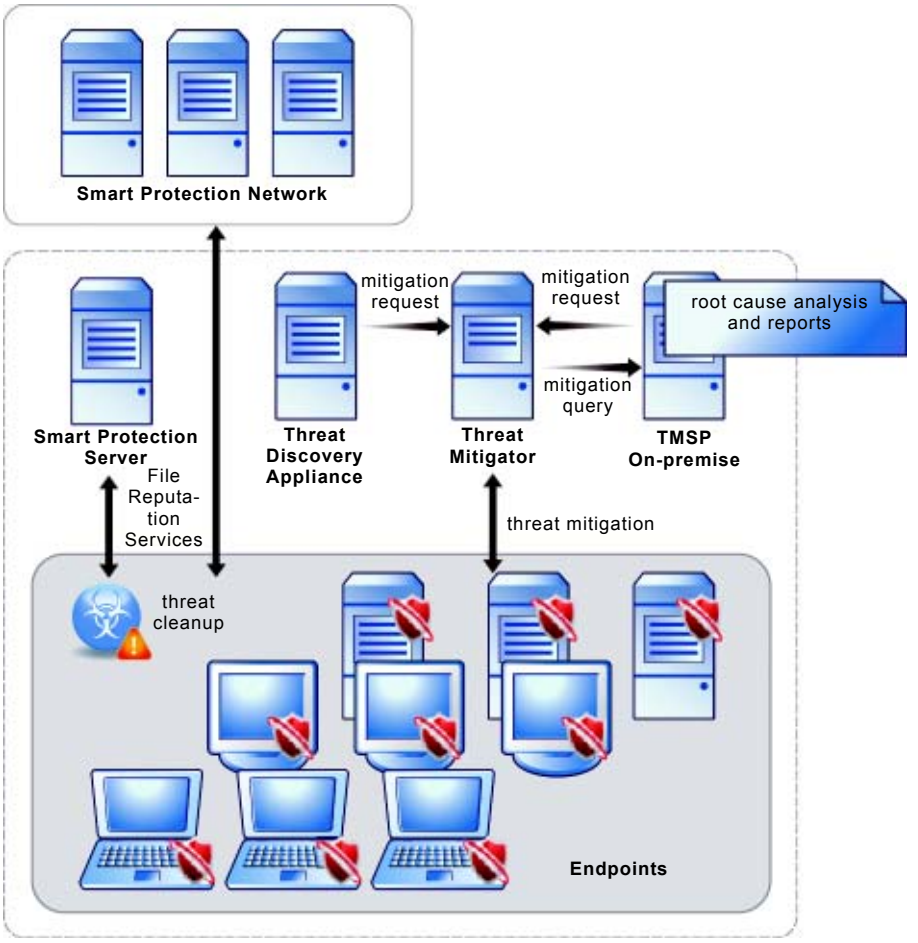


FIGURE 1-2. Threat mitigation process

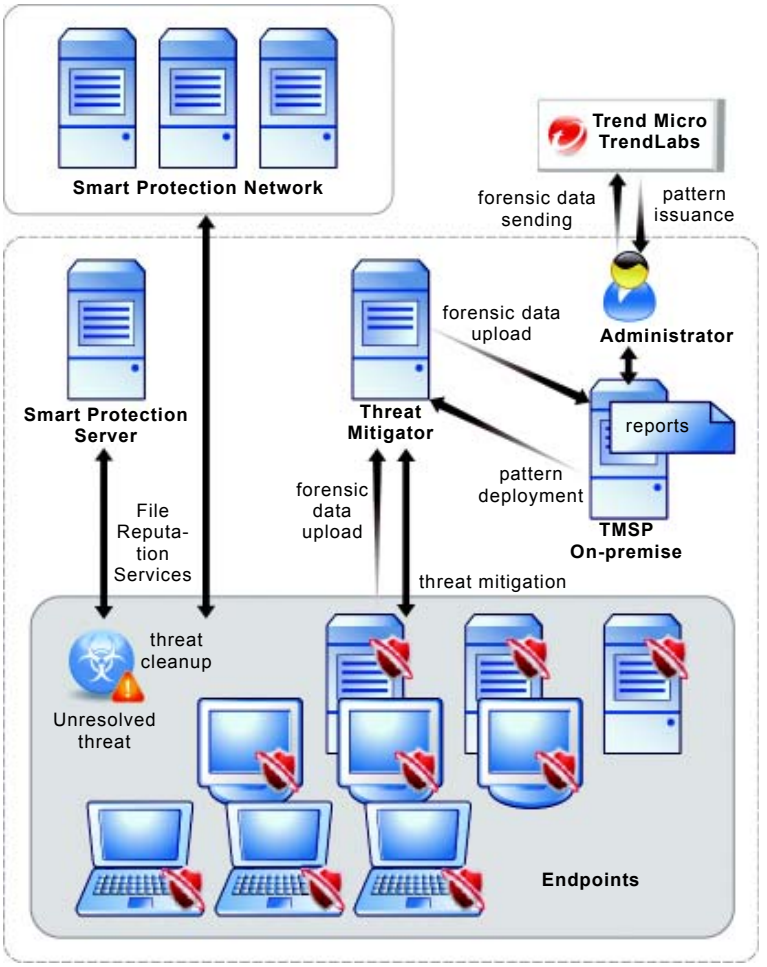


FIGURE 1-3. Advanced mitigation process

Chapter 2

Installation, Upgrade, and Uninstallation

This chapter guides you through the installation, upgrade, and uninstallation processes.

- If you are new to Threat Mitigator, perform a fresh installation of Threat Mitigator. See the following topics for installation notes and instructions:
  - *Threat Mitigator System Requirements* on page 2-3
  - *Pre-installation Guidelines* on page 2-4
  - *Threat Mitigator Fresh Installation* on page 2-8

Note: After installing Threat Mitigator, deploy Threat Management Agents using the deployment methods listed in *Agent Deployment Methods* on page 4-2.

- If you have previously installed Threat Mitigator, upgrade Threat Mitigator. After the upgrade, Threat Management Agents that report to Threat Mitigator automatically upgrade. For upgrade instructions, see *Threat Mitigator and Threat Management Agent Upgrades* on page 2-32.
- If you wish to uninstall Threat Mitigator, see *Threat Mitigator Uninstallation* on page 2-34.

Threat Mitigator System Requirements

Threat Mitigator requires the following resources:

TABLE 2-1. Threat Mitigator system requirements

RESOURCES	REQUIREMENTS
Host machine	• Memory: 2GB minimum • Processor: Intel™ Pentium™ 4, 2.4GHz or faster • Available disk space: 10GB recommended
Virtual machine	• Memory:768MB minimum • Processor: 2.4GHz or faster • Available disk space: 10GB recommended • Network adapter: At least one physical network adapter that connects to the network If there is a separate management network in your environment, Threat Mitigator requires another physical network adapter that connects to the management network.
Virtualization (minimum requirements)	• VMware™ ESX™/ESXi 4 with VMware vSphere™ Client • VMware ESX/ESXi 3.5 with VMware Infrastructure Client For VMware system requirements, refer to the VMware website: http://www.vmware.com/products/vi/esx/ **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.

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

RESOURCES	REQUIREMENTS
Browser	Microsoft™ Internet Explorer™ 6, 7, or 8 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

Threat Mitigator capacity is measured by the number of Threat Management Agents that can simultaneously send 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. By default, all agents send heartbeat messages at 15-minute intervals and start to do so each time they start up (typically, as a result of the agent's host computer starting up).

Note: The time interval for sending heartbeat messages is configured from Threat Mitigator's **Threat Mitigation > Agent Settings** screen.

In the capacity tests conducted by Trend Micro, the following were taken into consideration:

- The hardware resources on the Threat Mitigator host machine
- The number of agents that Threat Mitigator manages
- The time interval for sending heartbeat messages

Table 2-2 lists the resources used during the tests and the test results.

TABLE 2-2. Capacity test resources and results

CRITERIA	THREAT MITIGATOR WITH MINIMUM RESOURCES	THREAT MITIGATOR WITH RECOMMENDED RESOURCES
Host machine resources	• Intel Pentium 4, 2.4GHz • 2GB of memory • 1 core processor and 768MB of memory allocated to Threat Mitigator	• Dell™ PowerEdge™ 2950 • Intel™ Xeon™ X5355, 2.66GHz • 8GB of memory • 2 core processors and 2GB of memory allocated to Threat Mitigator
Maximum number of agents simultaneously sending heartbeat messages and time interval	1,000 agents at 10-minute intervals	1,000 agents at 2-minute intervals
	2,000 agents at 20-minute intervals	2,000 agents at 4-minute intervals
	5,000 agents at 52-minute intervals	5,000 agents at 10-minute intervals
	10,000 agents at 104-minute intervals	10,000 agents at 20-minute intervals
	20,000 agents at 208-minute intervals	20,000 agents at 40-minute intervals

The capacity tests show that a single Threat Mitigator server with either the minimum or recommended resources is capable of managing up to 20,000 agents. However, agents managed by a server with the recommended (or higher) resources can send heartbeat messages more frequently, which means that the required threat mitigation tasks can proceed without delay.

Trend Micro considers 15 minutes as the optimal time interval. In an extreme condition where a Threat Mitigator server with minimum resources manages 20,000 agents, a 208-minute interval may be too infrequent and unacceptable.

Therefore, if there are 5,000 endpoints in your organization and you have a high-performance host machine that meets the recommended requirements, a single Threat Mitigator server can manage agents on all the endpoints and you can keep the default time interval. If the host machine only has the minimum requirements, you will need to adjust the time interval to at least 60 minutes. If this time interval is not acceptable, prepare at least two Threat Mitigator servers, split the number of agents between the servers, and then reduce the time interval accordingly.

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 from the Threat Mitigator console, navigate to **Administration > Network Configuration > IP Address Settings**.

Threat Mitigator Fresh Installation

Threat Mitigator fresh installation involves the following tasks:

1. *Setting Up the VMware ESX/ESXi Server* on page 2-8
2. *Setting Up the VMware Client* on page 2-9
3. *Setting Up Threat Mitigator* on page 2-11

Note: If you are upgrading Threat Mitigator, see *Threat Mitigator and Threat Management Agent Upgrades* on page 2-32.

Setting Up the VMware ESX/ESXi Server

Threat Mitigator can be installed on a VMware ESX or ESXi server running on a host machine with the specifications listed in *Host machine* on page 2-3.

The VMware ESX/ESXi server is not included in the Threat Mitigator installation package. Visit the VMware website 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**.

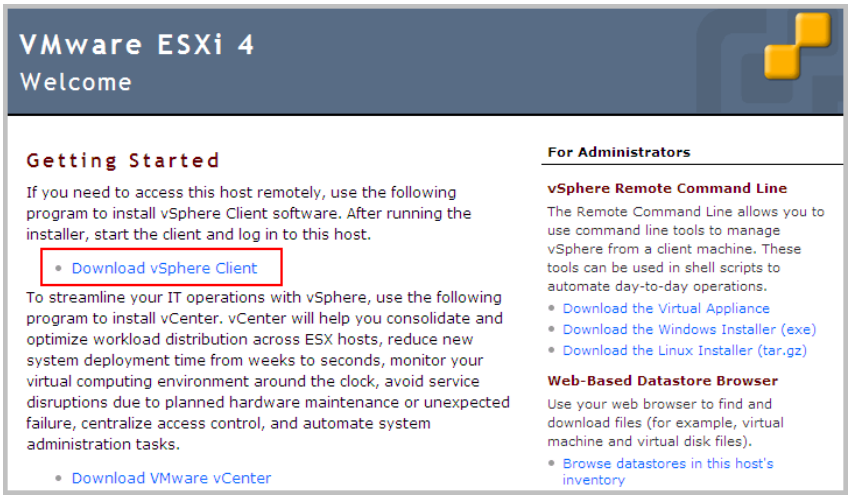


FIGURE 2-1. VMware ESX/ESXi 4.0 Welcome screen

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

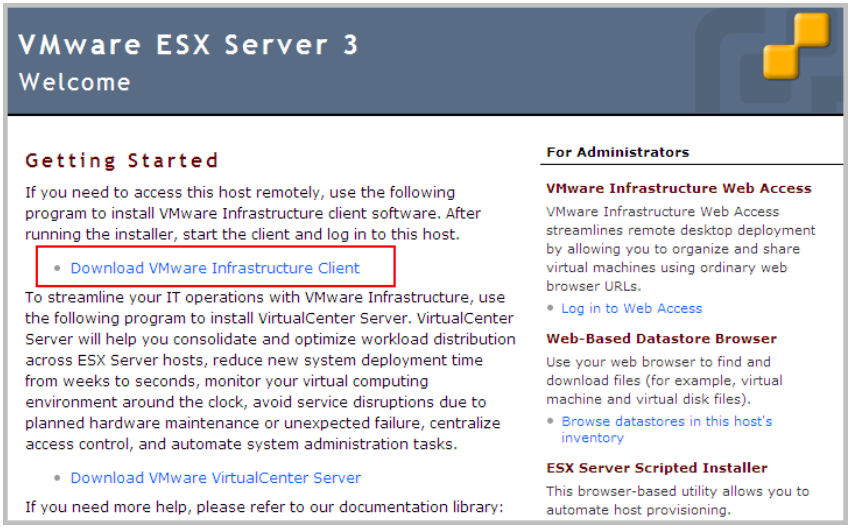


FIGURE 2-2. VMware ESX/ESXi 3.5 Welcome screen

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

The Threat Mitigator installation package is available for download from the Trend Micro website. 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 2-19.

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 screen

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

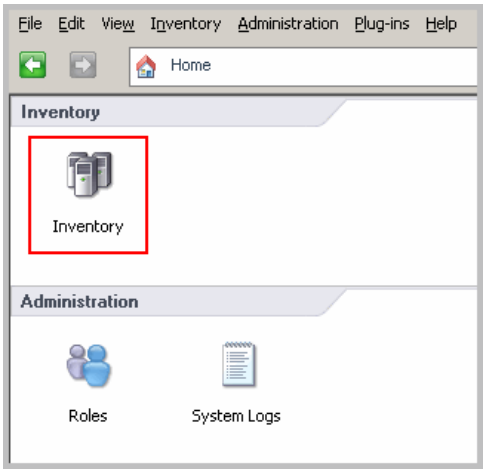


FIGURE 2-4. vSphere Client main screen

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**.

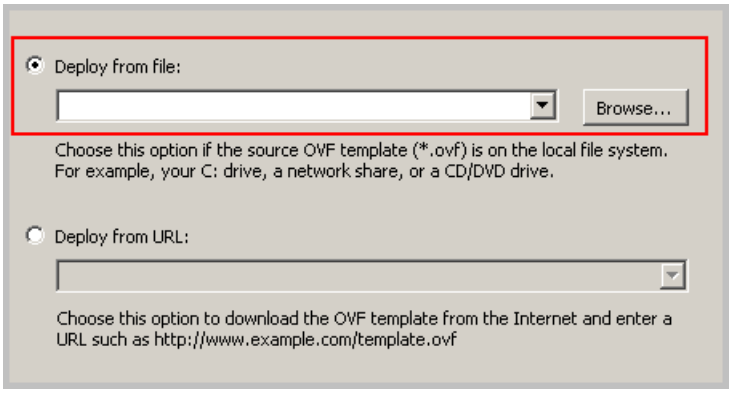


FIGURE 2-5. Deploy OVF Template screen

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.

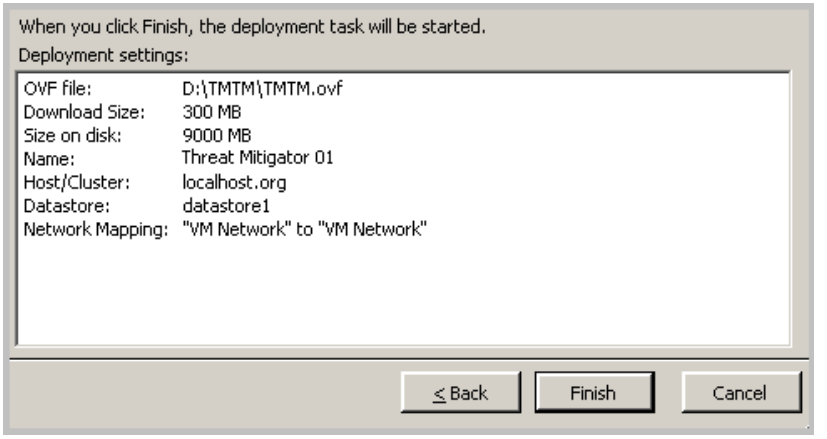


FIGURE 2-6. Ready to Complete screen

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**.

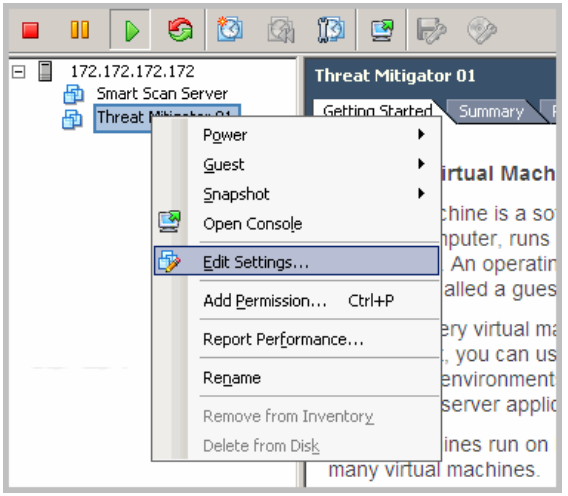


FIGURE 2-7. vSphere Client screen showing virtual machines

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

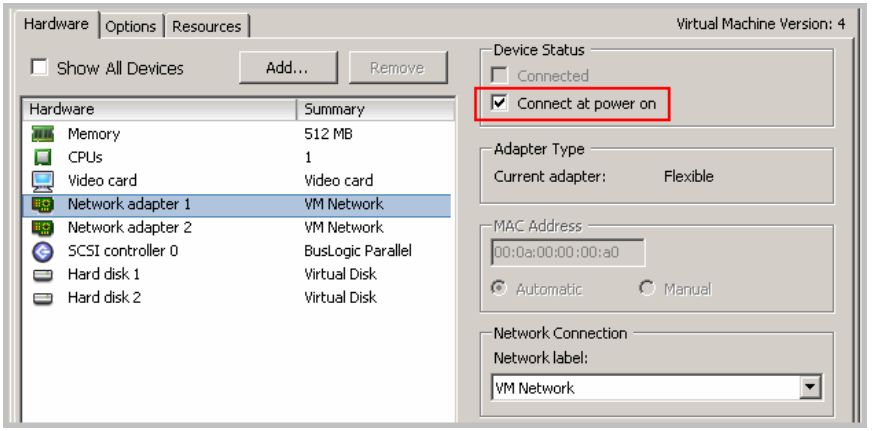


FIGURE 2-8. Network adapter 1 settings

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 **Connect at power on** options are enabled.

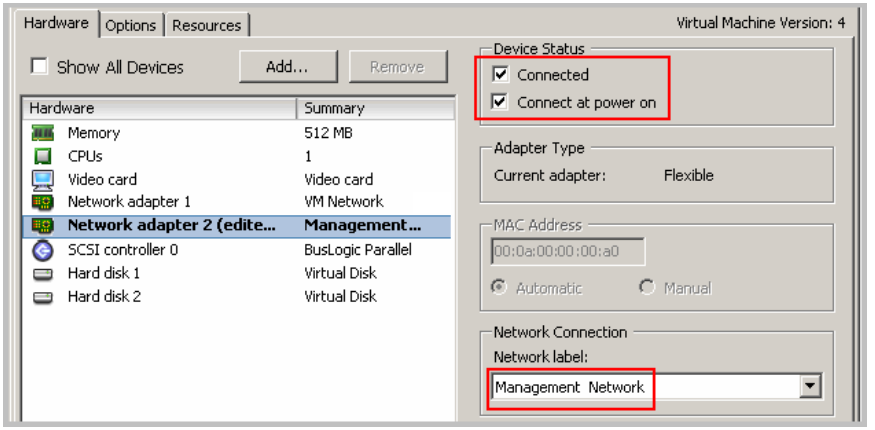


FIGURE 2-9. Network adapter 2 settings

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.

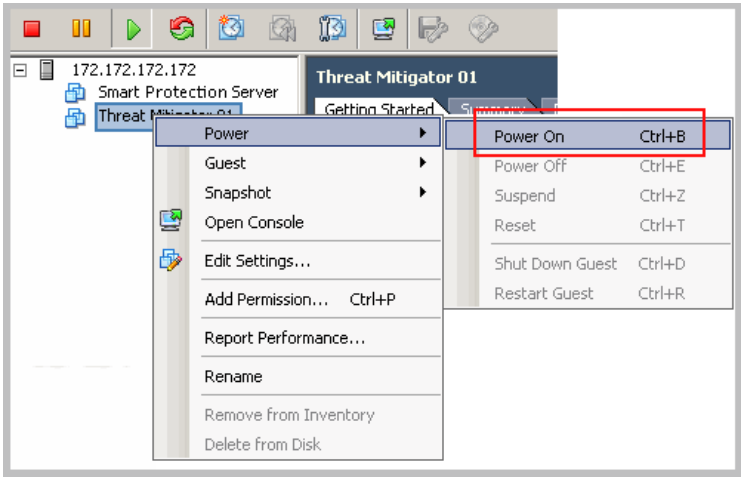


FIGURE 2-10. Power On option

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.

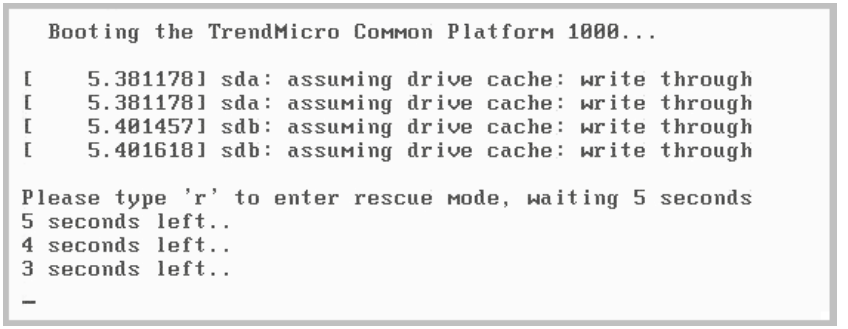


FIGURE 2-11. Threat Mitigator startup

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 2-28.

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 screen

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

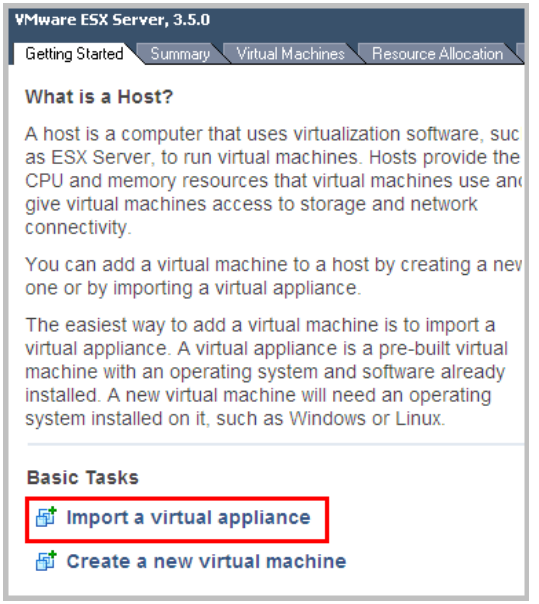


FIGURE 2-13. VMware Infrastructure Client main screen

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

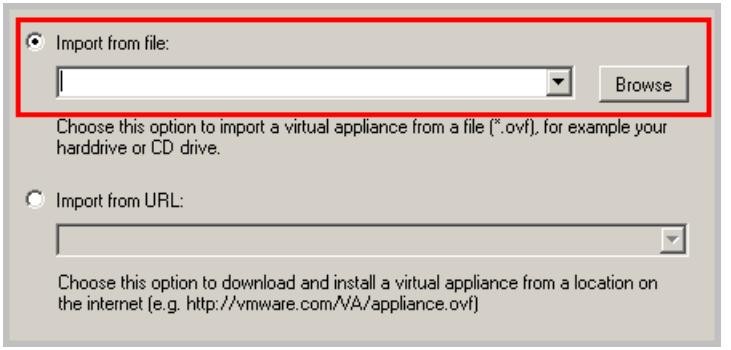


FIGURE 2-14. Import Location screen

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.

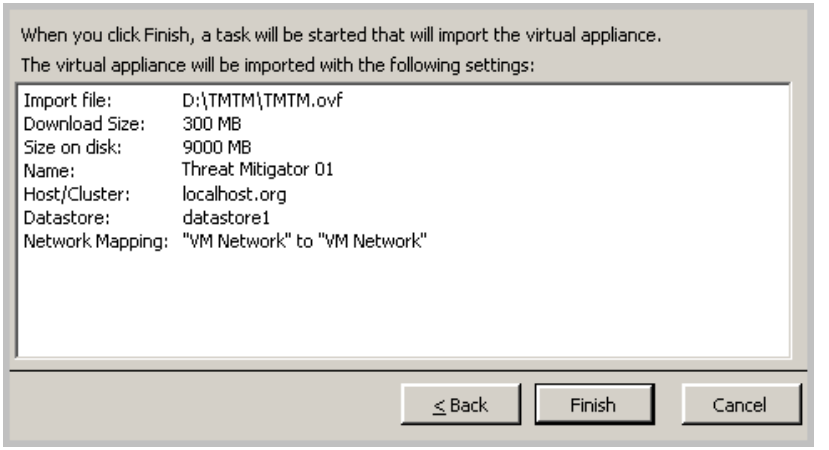


FIGURE 2-15. Ready to Complete Virtual Appliance Import screen

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**.

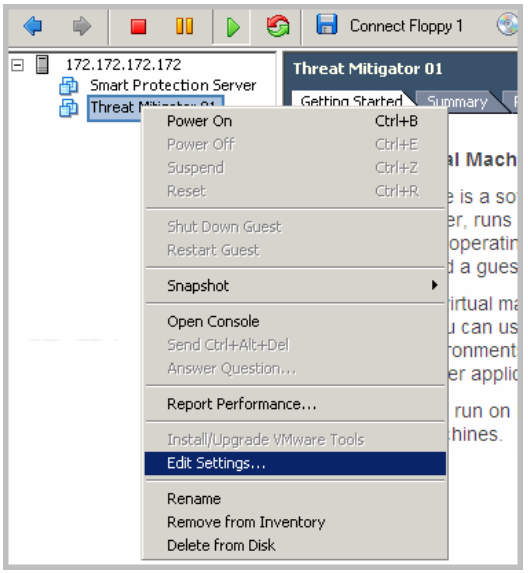


FIGURE 2-16. VMware Infrastructure Client screen showing virtual machines

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

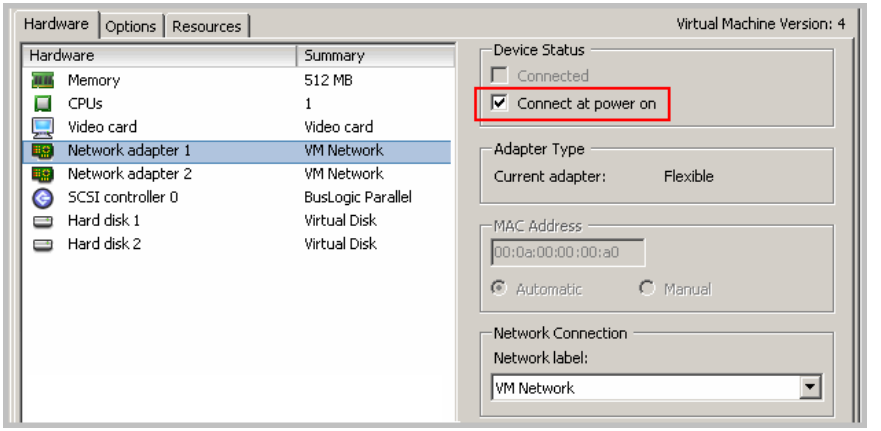


FIGURE 2-17. Network adapter 1 settings

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.

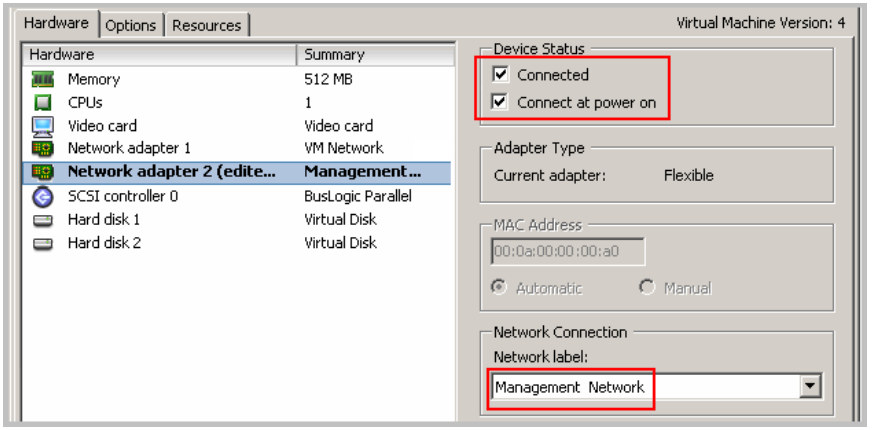


FIGURE 2-18. Network adapter 2 settings

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.

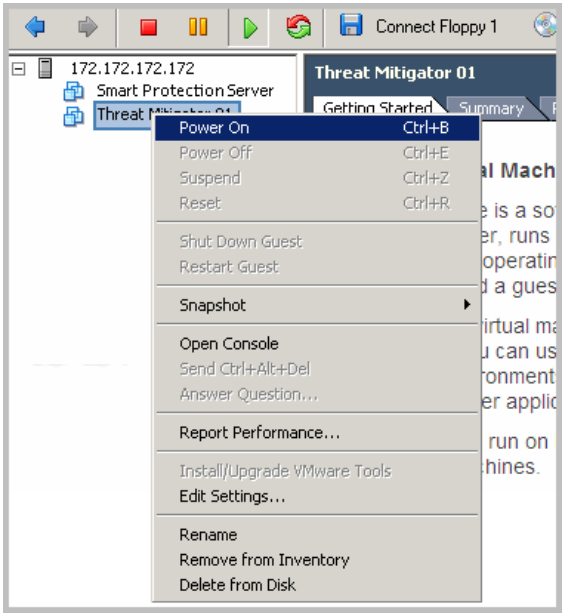


FIGURE 2-19. Power On option

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.

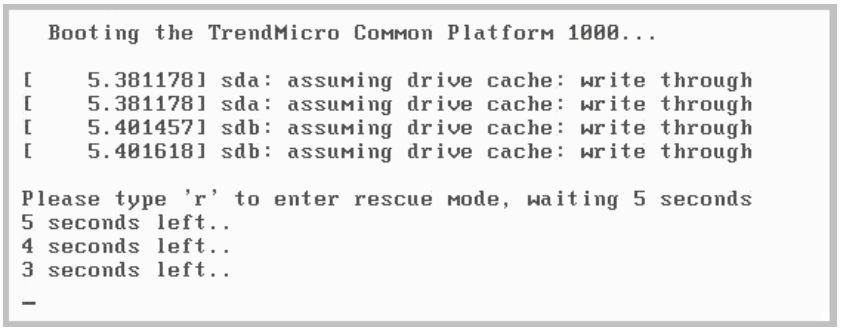


FIGURE 2-20. Threat Mitigator startup

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 2-28.

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 Protection Server (if one has been set up) require unique IP addresses. Check the IP addresses of the VMware ESX/ESXi server and Smart Protection 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 2-7.

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.

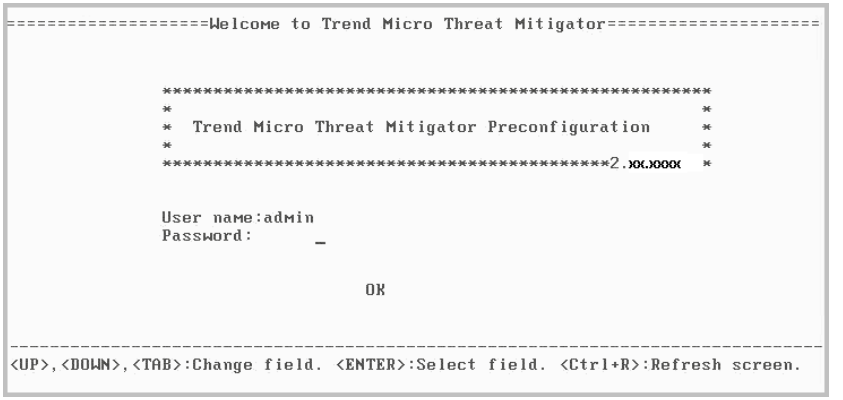


FIGURE 2-21. Welcome screen

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**.

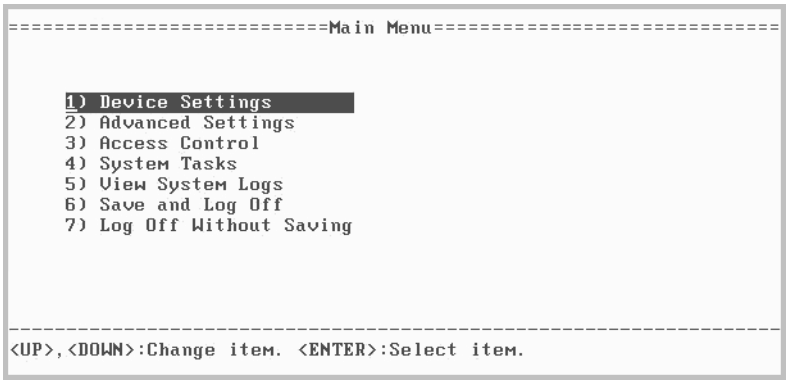


FIGURE 2-22. Main Menu screen with Device Settings highlighted

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)

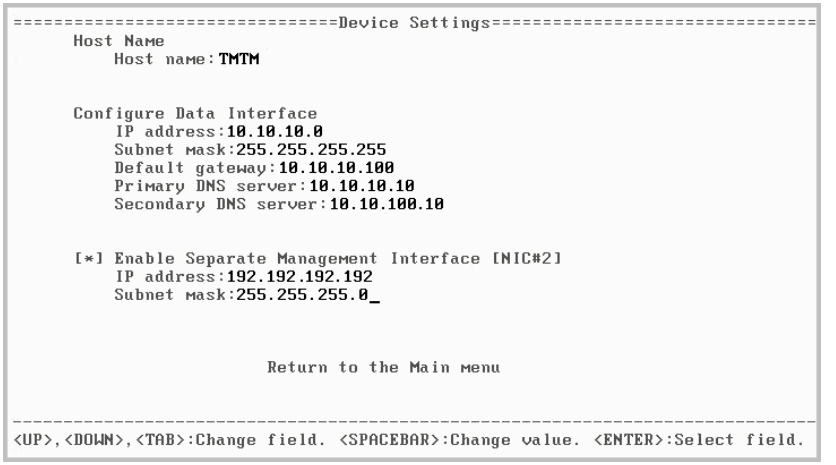


FIGURE 2-23. Device Settings screen

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**.

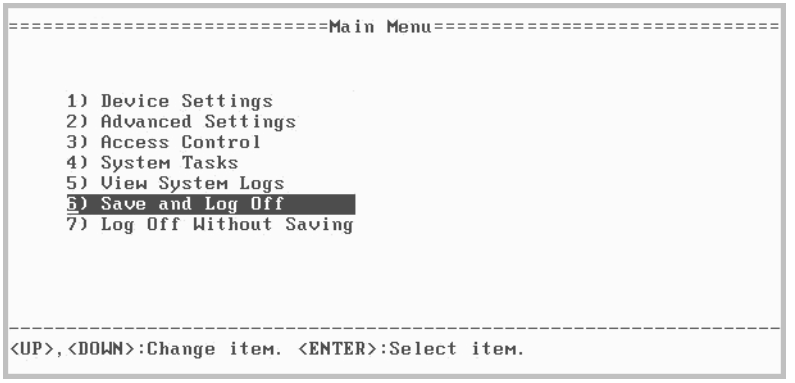


FIGURE 2-24. Main Menu screen with Save and Log Off highlighted

Note: After configuring the IP address, you can change it from the product console. For details, see *IP Address Settings* on page 8-10.

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 2-11 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 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, perform the following steps:

1. Unregister Threat Mitigator from Threat Discovery Appliance.
   a. On the Threat Discovery Appliance console, click **Mitigation > Mitigation Settings** in the main menu. The Mitigation Settings screen appears.
   b. Under **Registered Mitigation Devices**, select the Threat Mitigator IP address or sever name.
   c. Click **Delete**.
2. Uninstall Threat Management Agent from endpoints. For details, see *Agent Uninstallation* on page 4-30.
3. Uninstall Threat Mitigator from the VMware ESX server.
   a. Run the vSphere Client or the VMware Infrastructure Client.
   b. Log on to the VMware ESX server.
   c. Select Threat Mitigator from the list of virtual machines.
   d. 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**.
   e. Click **Inventory > Virtual Machine > Delete from Disk**.

Chapter 3

Getting Started

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

This chapter includes the following topics:

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. If your session has been inactive for a period of 600 seconds (10 minutes), the session terminates and you are automatically logged off from the console.

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 a provides 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 any screen at any time to log off from the console and return to the logon screen.

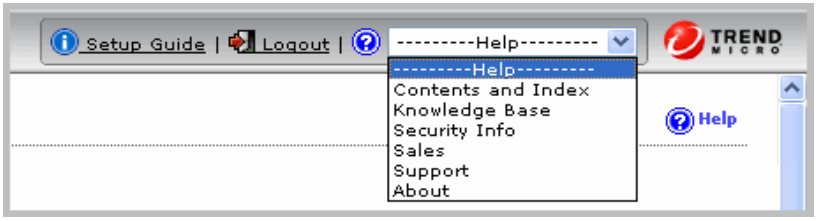


FIGURE 3-1. Product console banner

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

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

OPTION	DESCRIPTION
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)

OPTION	DESCRIPTION
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.

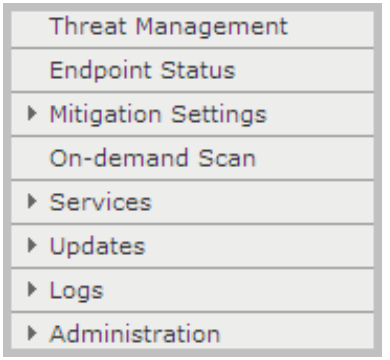


FIGURE 3-2. The main menu bar

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.

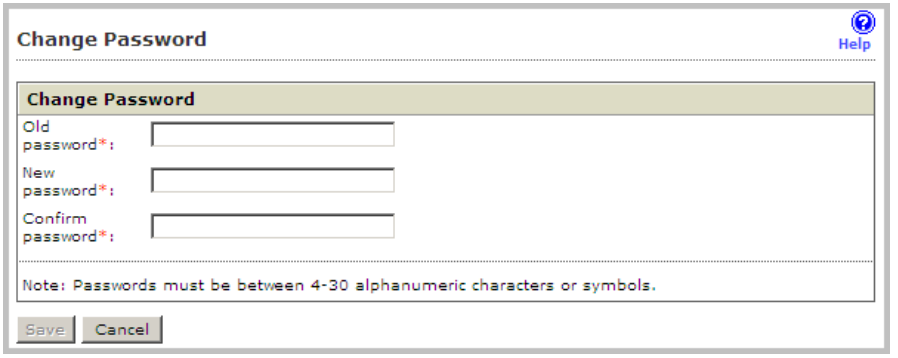


FIGURE 3-3. The main content window showing password settings

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**.

License and Activation Code

To use the functionality of Threat Mitigator, obtain an Activation Code and then activate the license. An Activation Code has 37 characters (including the hyphens) specified in the following format:

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

You can activate or renew the Threat Mitigator license in the Product License screen. Reminders will display during the following instances:

For a full version license:

- 30 days before expiration ends
- 30 days before grace period ends
- When the license expires and grace period elapses

> **Note:** After the grace period expires, you will not be able to obtain technical support and perform component updates. Threat Mitigator will still scan the network using out-of-date components. These out-of-date components may not be able to completely protect you from the latest security risks.

For an evaluation (trial) license:

- When the license expires

> **Note:** During this time, Threat Mitigator disables component updates, scanning, and log transmission to Threat Management Services Portal.

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 TMSP when prompted. For details, see *Threat Management Services Portal* on page 3-9.
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 website 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 > SYSTEM 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 7-20.

---

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

Threat Management Services Portal

Threat Management Services Portal (TMSP) receives logs and data from registered products and then issues targeted reports and custom solutions to product users. Register Threat Mitigator to TMSP to respond to threats in a timely manner and receive up-to-date information about the latest and emerging threats.

TMSP works with Threat Mitigator by:

- Receiving forensic data used for analyzing unresolved threats
- Deploying custom patterns to infected endpoints through Threat Mitigator to eliminate unresolved 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 TMSP periodically. A heartbeat message informs TMSP that Threat Mitigator is up and running and can therefore initiate threat mitigation tasks.

Note: Configure proxy settings if a proxy server is used to connect to TMSP. For details, see *Proxy Settings* on page 3-18.

Form Factor

TMSP is available as a Trend Micro hosted service, and as an on-premise application that you can install on a bare metal server or a virtual machine.

If you are installing the on-premise edition of TMSP:

- Refer to the TMSP *Administrator's Guide* for installation and configuration instructions.
- For information on the TMSP versions compatible with Threat Mitigator, see *Integration with Trend Micro Products and Services* on page 1-8.

If you have TMSP as a hosted service, ask your Trend Micro representative or support provider for the information required to register Threat Mitigator to TMSP. Information includes:

- IP addresses of TMSP's log server and status server
- Server authentication credentials

To configure TMSP settings:

PATH: SERVICES > THREAT MANAGEMENT SERVICES PORTAL

1. Select **Send logs and data to Threat Management Services Portal** to register Threat Mitigator to TMSP.

Note: If you disable this option, Threat Mitigator stops sending logs to TMSP and no longer downloads custom patterns from TMSP. The TMSP reports for Threat Mitigator will also not contain any data.

If you want to permanently disable this option, ensure that you unregister Threat Mitigator from TMSP by performing any of the following steps:

- If you have TMSP as an on-premise application, manually remove Threat Mitigator from TMSP's Registered Products screen.

- If you have TMSP as a hosted service, contact your Trend Micro representative about the unregistration.

---

2. Specify the log server for TMSP. The log server receives the following logs from Threat Mitigator:
   - **Threat event logs:** Threat Mitigator sends logs related to threat mitigation, including threat cleanup and custom pattern deployment. TMSP processes the logs and then lists endpoints with threat mitigation issues in the TMSP reports.
   - **Root cause logs:** Threat Mitigator sends logs that trace the root cause of infections. Information about the root cause of infections is also available in the TMSP reports.

   Perform any of the following steps:
   - If you have TMSP as a hosted service, type the IP address or host name of the log server.
   - If you have TMSP as an on-premise application, type the IP address of the log server.
3. Select the protocol. You can select either **SSH** or **SSL**.
4. Specify how often to send logs to TMSP.

5. Specify the status server for TMSP. The status server has the following functions:
   - Receives heartbeat messages from Threat Mitigator. Heartbeat messages inform TMSP that Threat Mitigator is up and running.
   - Receives forensic data from Threat Mitigator. For details about managing forensic data, see *Submit a Case* on page 5-18.
   - Stores the custom patterns issued by Trend Micro and notifies Threat Mitigator to download the required pattern. For details about custom patterns, see *Pattern Deployment and Custom Cleanup* on page 1-5.

   Perform any of the following steps:
   - If you have TMSP as a hosted service, type the IP address or host name of the status server.
   - If you have TMSP as an on-premise application, type the IP address of the status server.
6. Specify the upload or download bandwidth for the status server.
7. Type the server authentication credentials (user name and password). TMSP authenticates Threat Mitigator using these credentials and then proceeds to accept logs and data.
8. Type the registration email address.

   Tip: The email address is used for reference purposes. Trend Micro recommends typing your email address.

9. To check whether Threat Mitigator can connect to TMSP based on the settings you configured, 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
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 Protection Server to provide the same level of protection offered by conventional anti-malware patterns.
Damage Cleanup Engine	Scans endpoints for and repairs damage caused by malware. This engine can also check for vulnerabilities. **Tip:** Update this component only if you have security enforcement as part of your protection strategy.
Vulnerability Pattern	Contains information about vulnerabilities in popular software products and is used to identify vulnerabilities in endpoints **Tip:** Update this component only if you have security enforcement as part of your protection strategy.

TABLE 3-2. Threat Mitigator components (Continued)

COMPONENT	DESCRIPTION
Damage Cleanup Template	Contains cleanup information that is used by the Damage Cleanup Engine to identify malware and remove them from endpoints
Anti-rootkit Driver	Detects rootkits, sophisticated malware programs that are able to hide from Windows APIs and the detection tools that leverage them
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 Threat Discovery Appliance
Pattern Release History	Contains information about the latest patterns for supported antivirus products. Threat Mitigator uses this information to check whether endpoints are running the latest patterns. **Tip:** Update this component only if you have security enforcement as part of your protection strategy.
Antivirus Product Detection Engine	Scans endpoints to determine whether they are running supported antivirus software
Threat Management Agent	The program in the endpoint that: • Performs threat mitigation • Monitors endpoint security risk logs • Collects logs and forensic data

TABLE 3-2. Threat Mitigator components (Continued)

COMPONENT	DESCRIPTION
System Clean and Forensic Module	The module that: • 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
Program	The program software currently installed

Note: Threat Mitigator also downloads another type of pattern called **custom pattern**. This pattern is downloaded from TMSP and used only on specific endpoints where initial cleanup was unsuccessful. For details about custom patterns, see *Pattern Deployment and Custom Cleanup* on page 1-5.

Update Process

To update components successfully, perform the following tasks:

1. Configure the update source. For details, see *Update Source* on page 3-15.
2. If a proxy server is used to connect to the update source, configure proxy settings. For details, see *Proxy Settings* on page 3-18.
3. Perform a manual update. For details, see *Manual Updates* on page 3-16.
4. Configure an update schedule. For details, see *Scheduled Updates* on page 3-17.

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 2-7.

Update Source

Threat Mitigator downloads components from the Trend Micro ActiveUpdate server, the default update source. You can configure Threat Mitigator to download components from another update source, such as Trend Micro Control Manager.

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 3-18.
   - 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.
- **Scheduled Update:** Threat Mitigator automatically checks the update source at the frequency you specify.

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.

A separate section in the screen is provided for updating the Pattern Release History. Update this component only if you have security enforcement as part of your protection strategy.

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 number of minutes	Runs within the minute you specify, at the start time
Hours, every:	Every X number of hours	Runs within the hour you specify, at the start time
Days, every:	Every X number of days	Runs within the day you specify, at the start time
Weekly, every:	Every week, on a particular day	Runs weekly, on the day you specify, at the start time

3. Specify an update schedule for the Pattern Release History. See *Table 3-3* for the update frequency options.
4. Click **Save**.

Proxy Settings

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

- Connecting to TMSP
- 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 Protection Technology

Trend Micro smart protection technology is a next-generation, in-the-cloud based protection solution providing File and Web Reputation Services to endpoints. At the core of this solution is an advanced architecture that leverages threat signatures stored in-the-cloud.

Threat Mitigator leverages File Reputation Services during routine mitigation tasks and On-demand Scan.

Note: Threat Mitigator does not leverage Web Reputation Services.

In place of the conventional Virus Pattern, 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 Protection Server**. The File Reputation Services of Smart Protection Server process the query by checking the **Smart Scan Pattern**.

The Smart Scan Pattern hosted on the Smart Protection Server contains signatures not found in the Smart Scan Agent Pattern. This pattern checks whether the file is safe to access. A Smart Protection Server downloads and updates the Smart Scan Pattern from the Trend Micro ActiveUpdate server.

Endpoints that cannot connect to Smart Protection Server can send scan queries to **Trend Micro Smart Protection Network**. The following table provides a comparison between Smart Protection Server and Smart Protection Network.

TABLE 3-4. Smart protection sources

BASIS OF COMPARISON	TREND MICRO SMART PROTECTION NETWORK	SMART PROTECTION SERVER
Purpose	A globally scaled Internet-based infrastructure that provides File and Web Reputation Services to Trend Micro products that leverage smart protection technology	Provides the same File and Web Reputation Services offered by Smart Protection Network but is intended to localize these services to the corporate network to optimize efficiency
Administration	Trend Micro hosts and maintains this service.	Threat Mitigator administrators install and manage this server.
Connection protocol	HTTPS	HTTP/HTTPS

Smart Protection Implementation

Perform the following tasks to implement the smart protection solution in your security environment:

1. Install Smart Protection Server. For details, see *Smart Protection Server Installation* on page 3-20.
2. Configure Smart Protection Server settings from the Threat Mitigator console. For details, see *Smart Protection Server Settings* on page 3-20.

Smart Protection Server Installation

Install Smart Protection Server on a VMware server. Only one Smart Protection Server can be used in this Threat Mitigator version. For installation instructions and requirements, refer to the Installation and Upgrade Guide for Smart Protection Server.

Note: For information on the Smart Protection Server versions compatible with Threat Mitigator, see *Integration with Trend Micro Products and Services* on page 1-8.

Smart Protection Server, Threat Mitigator, and the VMware ESX/ESXi server (which hosts the Smart Protection 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 Protection Server.

If you have previously installed a Smart Protection Server for use with another Trend Micro product (such as Threat Discovery Appliance), you can use the same server for Threat Mitigator. While Smart Protection 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 Protection Server can handle scan queries coming from different products. Contact your support provider for sizing guidelines and recommendations.

Smart Protection Server Settings

After setting up a Smart Protection 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 Protection Server to send scan queries to the Trend Micro Smart Protection Network. Internet connection is required to connect to Smart Protection Network.

WARNING! **The mitigation task or On-demand Scan will not start if connection to both the Smart Protection Server and the Trend Micro Smart Protection Network 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 7-5.**

To configure Smart Protection Server settings:

PATH: SERVICES > SMART PROTECTION SERVER

1. Type the Smart Protection Server's address. You can find the address from the Smart Protection Server console's **Smart Protection > Reputation Services** screen.
2. Select the check box to allow endpoints to connect to the Trend Micro Smart Protection Network if connection to the Smart Protection Server cannot be established.
3. Click **Save**.

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.

You can also configure agents to run a scan immediately after it is installed to an endpoint.

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. Under **Post-installation Scan**:
   a. Select the check box to scan an endpoint for threats immediately after installing the agent.

b. 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

5. 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 4-6.

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 4-14.

Trend Micro Control Manager

Trend Micro Control Manager is a software management solution that gives you the ability to control antivirus and content security programs from a central location, regardless of the program's physical location or platform. This application can simplify the administration of a corporate antivirus and content security policy.

For information on the Control Manager versions compatible with Threat Mitigator, see *Integration with Trend Micro Products and Services* on page 1-8.

Refer to the Trend Micro Control Manager Administrator's Guide for more information about managing products using Control Manager.

Control Manager Components

Table 3-5 lists the components that make up Control Manager.

TABLE 3-5. Control Manager components

COMPONENT	DESCRIPTION
Control Manager server	The computer upon which the Control Manager application is installed. This server hosts the web-based Control Manager product console
Management Communication Protocol (MCP) Agent	An application installed along with Threat Mitigator that allows Control Manager to manage the product. The agent receives commands from the Control Manager server, and then applies them to Threat Mitigator. It also collects logs from the product, and sends them to Control Manager. The Control Manager agent does not communicate with the Control Manager server directly. Instead, it interfaces with a component called the Communicator.
Communicator	The communications backbone of the Control Manager system; it is part of the Trend Micro Management Infrastructure. Commands from the Control Manager server to Threat Mitigator, and status reports from Threat Mitigator to the Control Manager server all pass through this component.

TABLE 3-5. Control Manager components (Continued)

COMPONENT	DESCRIPTION
Entity	A representation of a managed product (such as Threat Mitigator) on the Control Manager console's directory tree. The directory tree includes all managed entities.

You can use the Control Manager Settings screen on the Threat Mitigator console to perform the following:

- Check the connection between Threat Mitigator and Control Manager
- Check the latest MCP heartbeat with Control Manager
- Register to a Control Manager server
- Unregister from a Control Manager server
- Verify that Threat Mitigator can register to a Control Manager server

Note: Ensure that both Threat Mitigator and the Control Manager server belong to the same network segment. If Threat Mitigator is not in the same network segment as Control Manager, configure the port forwarding settings for Threat Mitigator.

Control Manager Integration in this Release

The following features and capabilities are available when managing Threat Mitigator servers from Control Manager:

- **Configuration replication:** All configurable settings in Threat Mitigator can be replicated, except network configuration and product license settings.
- **Single sign-on:** Any Threat Mitigator account with administrator privileges can be used for single sign-on. The default account with administrator privileges is `admin`. To configure Threat Mitigator accounts, see *Administrative Accounts* on page 8-3.

Note: Accounts configured from Control Manager cannot be used for single sign-on.

- **Log submission:** Threat Mitigator sends system logs and system information to Control Manager. System information displays when you select Threat Mitigator from the Control Manager directory tree.
- **Component updates:** All updateable Threat Mitigator components can be deployed from Control Manager.

To register Threat Mitigator to Control Manager:

PATH: ADMINISTRATION > CONTROL MANAGER SETTINGS

1. Under **Connection Settings**, type the name that identifies Threat Mitigator in the Control Manager Product Directory.

   Note: Specify a unique and meaningful name to help you quickly identify Threat Mitigator.

2. Under **Control Manager Server Settings**:
   a. Type the Control Manager server IP address or host name.
   b. Type the port number that the MCP agent uses to communicate with Control Manager.
   c. If the Control Manager security is set to medium (Trend Micro allows HTTPS and HTTP communication between Control Manager and the MCP agent of managed products) or high (Trend Micro only allows HTTPS communication between Control Manager and the MCP agent of managed products), select **Connect using HTTPS**.
   d. If your network requires authentication, type the user name and password for your IIS server in the **Username** and **Password** fields.
3. If you want Threat Mitigator to connect to Control Manager through a proxy server:
   a. Select **Use a proxy server to communicate with the Control Manager server**.
   b. Select the proxy protocol.
   c. Type the server name or IP address and the port number.

d. If your proxy server needs authentication, type the user name and password in the fields provided.

4. If you use a NAT device, select **Enable two-way communication port forwarding** and type the NAT device's IP address and port number in **Port forwarding IP address** and **Port forwarding port number**. Threat Mitigator uses the **Port forwarding IP address** and **Port forwarding port number** for two-way communication with Control Manager.

Note: Configuring the NAT device is optional and depends on the network environment.

---

5. To check whether Threat Mitigator can connect to the Control Manager server based on the settings you specified, click **Test Connection**.
6. Click **Register** if connection was successfully established.

To check the Threat Mitigator status on the Control Manager console:

1. Open the Control Manager management console.

   To open the Control Manager console, on any computer on the network, open a web browser and type the following:

   https://<Control Manager server name>/Webapp/login.html

   Where <Control Manager server name> is the IP address or host name of the Control Manager server
2. In Main Menu, click **Products**.
3. Locate Threat Mitigator in the Product Directory. You can use Directory Management to move Threat Mitigator to the correct location in the Product Directory.

To manage the connection with Control Manager after registration:

PATH: ADMINISTRATION > CONTROL MANAGER SETTINGS

1. Under **Connection Status**, do the following:
   - Check if the product can connect to Control Manager. If the product is not connected, restore the connection immediately.

- Check the last heartbeat, which indicates the last communication between the MCP agent (and Threat Mitigator) and the Control Manager server.

2. If you change any of the settings after registration, click **Update Settings** to notify the Control Manager server of the changes.
3. If you want another Control Manager server to manage Threat Mitigator, click **Unregister** and then register Threat Mitigator to the other server.

Chapter 4

Deploying Threat Management Agents

This chapter guides you through the Threat Management Agent deployment process.

This chapter includes the following topics:

Note: To upgrade Threat Management Agents from a previous version, see *Threat Mitigator and Threat Management Agent Upgrades* on page 2-32.

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	The Packager tool creates an agent package in Microsoft Installer (MSI) format. After creating the package, you can deploy it to endpoints through the Trend Micro Endpoint Security Plafform, Active Directory, Microsoft SMS, or other software deployment applications. For details, see *Agent Deployment Using the Packager Tool* on page 4-6.
Browser-based installation	Provide users with a link that launches the agent installation program from an Internet Explorer browser window. For details, see *Agent Deployment Using Browser-based Installation* on page 4-14.
Using TMAgent Manager	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. For details, see *Agent Deployment Using TMAgent Manager* on page 4-16.

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 3-22.

Agent Requirements

To deploy Threat Management Agent, the endpoint must have the following resources:

TABLE 4-2. Agent system requirements

RESOURCE	REQUIREMENTS
Operating system	• 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 • Windows 7 (32-bit version)
Processor	At least 133 MHz Intel™ Pentium™ (or equivalent)
Memory	64MB minimum, 256MB recommended
Available hard disk space	620MB minimum

Additional Requirements - Packager Tool

A computer that can access the Threat Mitigator console is required. The tool will be downloaded to a folder on this computer.

Additional Requirements - Browser-based Installation

Microsoft™ Internet Explorer™ 6, 7, or 8 is required to launch the installation.

Additional Requirements - TMAgent Manager

Earlier versions of TMAgent Manager are available from the ActiveUpdate server. However, this version is not. You need to use the **standalone installation package** to install or upgrade TMAgent Manager.

The following items are required when deploying the agent using TMAgent Manager.

For TMAgent Manager:

- A computer with the following programs already installed and currently running:
  - OfficeScan server, version 8.0 Service Pack 1 or later
  - In some OfficeScan server versions, TMAgent Manager cannot retrieve the correct OfficeScan domain and client information from the OfficeScan server database. To resolve this issue, apply the following OfficeScan hot fixes:
    - For OfficeScan 10 Service Pack 1: Hot fix 1791.3
    - For OfficeScan 8 Service Pack 1 with Patch 4: Hot fix 3450
  - Plug-in Manager server, version 1.0 (apply the latest patch, if available)
- 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.

For Threat Management Agent and TMAgent Manager client:

- A computer with the following programs already installed and currently running:
  - OfficeScan client, version 8.0 Service Pack 1 (or later version)
  - Plug-in Manager client, version 1.0

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.

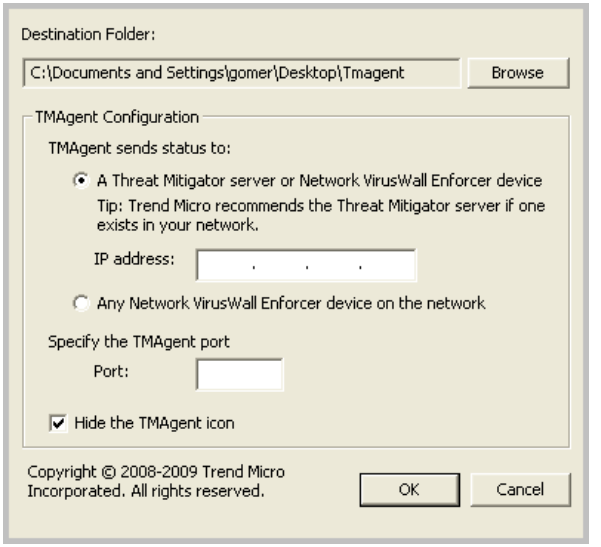


FIGURE 4-1. Packager tool

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:

- From Trend Micro Endpoint Security Platform. For details, see *Package Deployment Using Endpoint Security Platform* on page 4-8.
- Through Active Directory. For details, see *Package Deployment Using Active Directory* on page 4-10.
- Through Microsoft SMS (or other software deployment applications). For details, see *Package Deployment Using Microsoft SMS* on page 4-11.
- 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 4-13.
- By copying the package to a shared folder accessible to users. For details, see *Package Deployment Using a Shared Folder* on page 4-13.
- By launching the package directly on the target computer

Package Deployment Using Endpoint Security Platform

Trend Micro Endpoint Security Platform (ESP) aims to solve the increasingly complex problem of keeping critical systems updated, compatible, and free of security leaks. It uses patented Fixlet™ technology to identify vulnerable computers and allows you to remediate them across your entire network with a few simple mouse-clicks.

To deploy the agent successfully, ensure that the ESP Client has been deployed to each target endpoint. The ESP Client accesses a collection of Fixlet messages that detects security holes, improper configurations and other vulnerabilities. The ESP Client is then capable of implementing corrective actions received from the ESP Server.

After deploying the agent, the agent reports its status to its parent server and the ESP server. The agent also begins to receive threat mitigation requests from its parent server.

For endpoints that are not up and running during agent deployment, the agent will automatically be deployed when the endpoint is started and if the agent deployment task has not expired. Run the task again if it has expired.

To deploy the agent from the ESP server's console:

Note: Refer to the ESP server documentation for the detailed procedures.

---

1. (Recommended) Create a custom analysis that queries endpoints that do not have Threat Management Agent installed. One of the ways to determine the presence of the agent is by checking if the following registry key exists:

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

2. Create a task that silently deploys the agent to target endpoints. When you create this task:

   a. Select only the Windows operating systems listed in *Agent Requirements* on page 4-3.

   b. To generate an MSI log file that can be used for troubleshooting agent deployment issues, use the following string:

      ```
      msiexec /i PEAgent.msi /qn ALLUSERS=1 /lv msi.log
      ```

The following is a sample script for this task:

Relevance:

```
(name of it = "Win2000" OR name of it = "WinXP" OR name of it =
"Win2003" OR (name of it = "WinVista" and product type of it =
nt workstation product type) OR (name of it = "Win2008" or (name
of it = "WinVista" and product type of it != nt workstation
product type))) of operating system AND TRUE AND (if (exists
file "msiexec.exe" of system folder) then true else false) AND
(if (exists key
"HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" whose
(exists value "ApplicationPath" of it) of registry) then FALSE
else TRUE)
```

Actions:

```
download
http://x.x.x.x:52311/Uploads/c2790100fb90aba4c9596709586009b590
dec4a7/PEAgentmsi.tmp

continue if {(size of it = 4739051 AND sha1 of it =
"c2790100fb90aba4c9596709586009b590dec4a7") of file
"PEAgentmsi.tmp" of folder "__Download"}

extract PEAgentmsi.tmp

wait "{pathname of system folder & "\msiexec.exe"}" /i
"{(pathname of client folder of current site) &
"\__Download\PEAgent.msi"}" /qn ALLUSERS=1 /lv msi.log
```

Note: The download URL is based on the URL used in the ESP Agent Import wizard.

3. Verify that the agent was installed successfully. For details, see *Agent Post-installation* on page 4-26.

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.
8. Verify that the agent was installed successfully. For details, see *Agent Post-installation* on page 4-26.

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.
19. Verify that the agent was installed successfully. For details, see *Agent Post-installation* on page 4-26.

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 msiexec /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.

After the deployment, verify that the agent was installed successfully. For details, see *Agent Post-installation* on page 4-26.

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.

After the deployment, verify that the agent was installed successfully. For details, see *Agent Post-installation* on page 4-26.

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

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

Agent Settings screen (Mitigation Settings > Agent Settings)

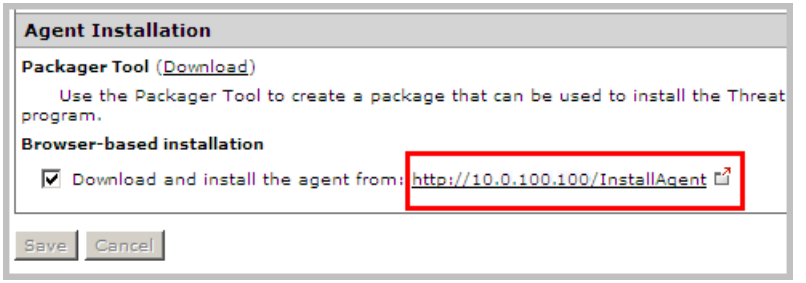


FIGURE 4-3. Agent installation link on the Agent Settings screen

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.

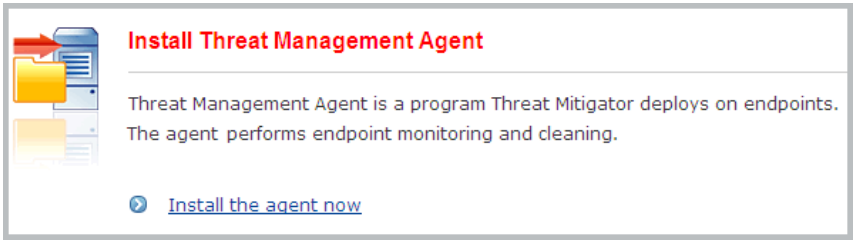


FIGURE 4-4. Browser-based installation screen

   b. Click **Install the agent now** to start the installation. The installation status and result display on the same screen.
3. Verify that the agent was installed successfully. For details, see *Agent Post-installation* on page 4-26.

Agent Deployment Using TMAgent Manager

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.

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 discussed in *Agent Deployment Methods* on page 4-2.

TMAgent Manager Components

TMAgent Manager consists of the following programs:

- TMAgent Manager
- Threat Management Agent
- TMAgent Manager client

TMAgent Manager

TMAgent Manager is a program installed on the same computer that hosts the OfficeScan server and Plug-in Manager. Once installed, this program can deploy Threat Management Agent to endpoints.

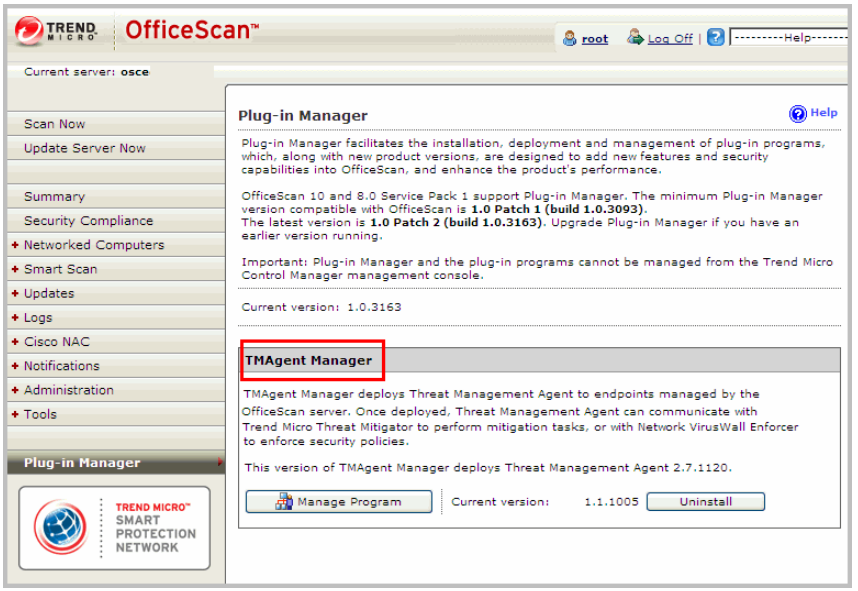


FIGURE 4-5. Plug-in Manager console, with TMAgent Manager highlighted

Threat Management Agent

Threat Management Agent is an endpoint-based program that receives and then acts on mitigation requests from Threat Mitigator. Threat Management Agent runs routine mitigation tasks (such as assessing the endpoint's security posture, running cleanup, and collecting forensic data if cleanup was unsuccessful) and reports the mitigation status to Threat Mitigator.

Note: TMAgent Manager only deploys Threat Management Agent to endpoints. It cannot send mitigation requests to the agents.

Threat Management Agent can also communicate with Network VirusWall™ Enforcer to enforce security policies on the endpoint.

TMAgent Manager client

TMAgent Manager client is an endpoint-based program that serves as the communication channel between Threat Management Agent and TMAgent Manager.

TMAgent Manager client displays on the OfficeScan client's Plug-in Manager screen. It runs mostly in the background and does not have settings that endpoint users need to configure.

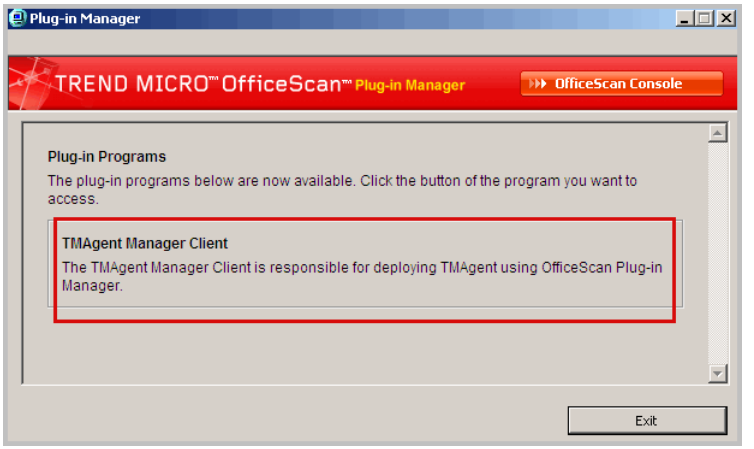


FIGURE 4-6. TMAgent Manager client displayed on the OfficeScan client's Plug-in Manager screen

TMAgent Manager client and Threat Management Agent are installed together. You do not need to run two separate installations. When you launch agent deployment from TMAgent Manager, the installation package first installs TMAgent Manager client, followed by Threat Management Agent. The agent will not be installed if there are problems installing TMAgent Manager client.

The installation path for TMAgent Manager client is `%ProgramFiles%\Trend Micro\PEAgentManagerClient`.

The installation path for Threat Management Agent is `%WINDIR%\PEAgent`.

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

Install TMAgent Manager using the standalone installation package (in `.msi` file format), which is available in version 1.1 (and later versions) of TMAgent Manager. The package supports all language versions supported by OfficeScan. You can obtain the package from the Trend Micro website or from your Trend Micro representative.

Installation guidelines and reminders:

1. See *Agent Requirements* on page 4-3 for a list of requirements needed to install TMAgent Manager successfully.
2. The installation package for this TMAgent Manager version is not available on the Trend Micro ActiveUpdate server, and therefore cannot be downloaded and launched from the Plug-in Manager screen. If you see the TMAgent Manager section with a **Download** button in the Plug-in Manager screen, the package to be downloaded is for an earlier product version (1.0.xxxx). The earlier version is NOT required to install this product version.
3. If you have an earlier version of TMAgent Manager already installed, the **Download** button will not be available in the Plug-in Manager screen. Launch the standalone installation package to upgrade TMAgent Manager.
4. Launch the installation from the computer that hosts the OfficeScan server and Plug-in Manager. TMAgent Manager will not be installed if you launch the installation on another computer.
5. After the installation, a separate TMAgent Manager console is created and can be opened from within the OfficeScan server and the Plug-in Manager consoles. The TMAgent Manager console can be accessed from any computer on the network.

To install TMAgent Manager:

1. Copy the installation package to any directory on the computer that hosts the OfficeScan server and Plug-in Manager.
2. Launch the package. The InstallShield Wizard opens.
3. Click **Next**.
4. Agree to the terms of the license agreement and then click **Next**. The installation process starts.

5. If you encounter installation problems, collect the following logs:
   - OfficeScan server debug logs (refer to the OfficeScan server documentation for log collection instructions)
   - MSI installation logs. To collect logs, execute the following command from the command-line interface:
     - On computers running Windows Server 2000, or computers with Windows Installer 2.0 installed:

       ```
       Msiexec /i PEAMSrvPackage.msi /lv install.log
       ```

     - On computers running Windows XP or later operating systems, or computers with Windows Installer 3.0 installed:

       ```
       Msiexec /i PEAMSrvPackage.msi /lvx install.log
       ```

6. When the installation completes, click **Finish**.

TMAgent Manager Client Tree

PATH: OFFICESCAN SERVER CONSOLE > PLUG-IN MANAGER > MANAGE PROGRAM

The main screen in the TMAgent Manager console displays the TMAgent Manager client tree.

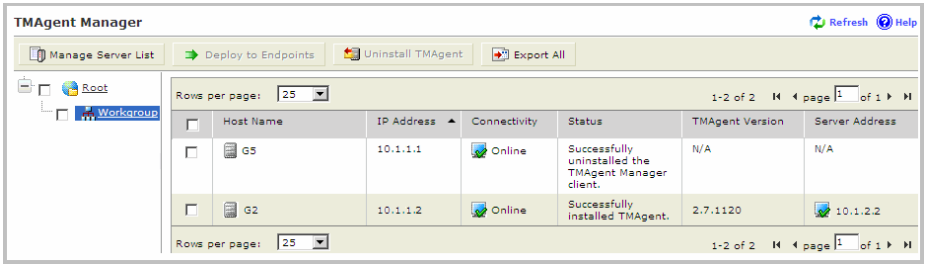


FIGURE 4-7. The TMAgent Manager client tree

The TMAgent Manager client tree and the OfficeScan server's client tree are identical. This means that:

- Any changes in the OfficeScan server's client tree (such as moving clients from one domain to another) will also be reflected in the TMAgent Manager client tree.
- OfficeScan clients are installed on all the endpoints listed in theTMAgent Manager client tree and are being managed by the OfficeScan server. However, Threat Management Agent may or may not be installed on the endpoints.

Tip: See the **TMAgent Version** column in the client tree to determine whether the agent is installed on the endpoint. "N/A" displays if the agent is not installed.

The following endpoints do not appear in the TMAgent Manager client tree, even if Threat Management Agent is installed on these endpoints:

- An endpoint with OfficeScan client managed by another OfficeScan server
- An endpoint with an unmanaged OfficeScan client (the client does not report to any OfficeScan server)
- An endpoint without OfficeScan client

Client Tree Information

The client tree displays the following items and information:

- **The "root" directory:** Found on the left side of the screen and contains a list of domains beneath it. Each domain contains a list of endpoints.
- **Host Name:** The endpoint's host name
- **IP Address:** The endpoint's IP address
- **Connectivity:** The endpoint's connection status with the OfficeScan server (Online, Offline, or Roaming)

  Note: The connection status of Threat Management Agent with its parent server (Threat Mitigator or Network VirusWall Enforcer) is indicated in the **Server Address** column.

- **Status:** The status of the most recent task performed on the endpoint

- **TMAgent Version:** The version of Threat Management Agent installed on the endpoint. "N/A" displays if the agent is not installed.
- **Server Address:** The IP address of the Threat Mitigator or Network VirusWall Enforcer server to which the agent communicates.
  - If the agent communicates with multiple servers, the IP addresses of all the servers display.
  - A green check mark in the icon before the IP address indicates that the agent can connect to the server. A red "x" mark indicates that connection cannot be established.
  - "N/A" displays if the agent is not installed on the endpoint.

TMAgent Manager Server List

After setting up one or several Threat Mitigator servers, add the servers to the TMAgent Manager Server List. When you deploy Threat Management Agent, you will be prompted to select the server from which the agent will receive mitigation requests and report its status.

You can also add Trend Micro Network VirusWall Enforcer™ to the list, if one has been set up. Threat Management Agent can report its status to both Threat Mitigator and Network VirusWall Enforcer. These two products share common features (such as endpoint cleanup) and feature conflicts may arise when the agent reports to both products. To avoid feature conflicts, refer to the checklist provided in *Network VirusWall Enforcer Installations* on page 2-7.

To manage the server list:

PATH: OFFICESCAN SERVER CONSOLE > PLUG-IN MANAGER > MANAGE PROGRAM > MANAGE SERVER LIST

1. Specify Threat Mitigator's IP address, description, and port number in the fields provided. Repeat this step to add Network VirusWall Enforcer servers.

   You can obtain the IP address and port number from the product console.

   For Threat Mitigator:

   - **IP address:** Navigate to **Administration > Network Configuration > IP Address Settings**.
   - **Port number:** Navigate to **Mitigation Settings > Agent Settings** and go to the **Communication Port** section.

   For Network VirusWall Enforcer:

   - **IP address:** Navigate to **Administration > IP Address Settings**.
   - **Port number:** Navigate to **Policy Enforcement > TMAgent Settings** and go to the **Threat Management Agent Settings** section.

   Note: You can also view the IP address for both Threat Mitigator and Network VirusWall Enforcer from the preconfiguration console by selecting the **Device Settings** menu item.

2. Click **Add Server**. The server name and address appears in the server list.
3. To remove a server from the list, click the trash bin icon  .

   Note: This action only removes the server from the list, which means that the server will no longer display the next time you deploy the agent to a new endpoint. The server is not uninstalled and continues to manage the agents already reporting to it.

Agent Deployment from the TMAgent Manager Console

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**. You can check the deployment status from the TMAgent Manager console.

Note: Threat Management Agent will not be installed if there are problems installing TMAgent Manager client.

When the 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 the TMAgent Manager console:

PATH: OFFICESCAN SERVER CONSOLE > PLUG-IN MANAGER > MANAGE PROGRAM > DEPLOY TO ENDPOINTS

1. Select the endpoints to which to deploy the agent.
   - 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.

   - 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.

3. Choose from the following options:
   - **Deploy default TMAgent settings:** Deploys Threat Management Agent without registering it to a specific parent server. When the agent detects a Network VirusWall Enforcer or Threat Mitigator server, it automatically registers to that server.
   - **Select Threat Mitigator server:** Deploys Threat Management Agent and registers it to a specific Threat Mitigator server. The servers that display are configured from the Manage Server List screen. For details about the server list, see *TMAgent Manager Server List* on page 4-23.
4. 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.
5. Verify that the agent was installed successfully. For details, see *Agent Post-installation* on page 4-26.

Agent Post-installation

Verify the following after deploying agents:

1. The agent icon  appears on the endpoint's system tray after the agent registers to its parent server.

Note: An option in the Threat Mitigator console (in the **Mitigation Settings > Agent Settings** screen) can hide the agent icon from view. If this option is enabled on the Threat Mitigator server to which the agent reports, the icon will not display in the system tray.

If the agent icon is not visible, refer to the other checkpoints below to verify that the agent has been installed successfully.

---

2. The agent program exists in `%WINDIR%/PEAgent`.
3. The agent registry key exists.

   `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Policyenforcer`

4. 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.
   - The Network VirusWall Enforcer console's Summary screen
5. If the agent was deployed from TMAgent Manager:
   a. The agent version and the server (Threat Mitigator or Network VirusWall Enforcer) to which the agent reports are displayed on the TMAgent Manager console.
   b. On the endpoint, the TMAgent Manager Client program exists in %ProgramFiles%\Trend Micro\PEAgentManagerClient.
   c. On the endpoint, the TMAgent Manager Client registry key exists: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PEAgentManager Client.
   d. On the endpoint, the the TMAgent Manager Client program is available on the Plug-in Manager screen on the OfficeScan client 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 3-22.
2. If you deployed the agent from the Endpoint Security Platform console, create an analysis that collects the following information from endpoints:
   - Agent version
   - Agent installation time
   - Whether the agent service is up and running
   - Agent's parent server and communication port
   - Agent's installation path

The following is a sample script for this analysis:

```
Property Name="Trend Micro Threat Management Agent Version"

if (exists key
"HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" of
registry) then (value "Version" of key
"HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" of
registry as string) else "N/A"

Property Name="Trend Micro Threat Management Agent Installation
Time"

if (exists key
"HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" of
registry) then (value "InstallDate" of key
"HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" of
registry as string) else "N/A"

Property Name="Trend Micro Threat Management Agent Status"

if (exists running service "TMAgent")then ("Running") else ("Not
Running")

Property Name="Trend Micro Threat Management Agent Registered
Server's IP:Port"

if (exists key
"HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" of
registry) then (value "Reportto" of key
"HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" of
registry as string) else "N/A"

Property Name="Trend Micro Threat Management Agent Installed
Directory"

if (exists key
"HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" of
registry) then (value "ApplicationPath" of key
"HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" of
registry as string) else "N/A"
```

Relevance:

```
(((if( name of operating system starts with "Win" ) then
platform id of operating system != 3 else false) AND (name of
operating system as lowercase starts with "win")) AND (version
of client >= "5.0")) AND (if (exists key
"HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" whose
(exists value "ApplicationPath" of it) of registry) then TRUE
else FALSE)
```

3. If you deployed the agent from the Endpoint Security Platform console, create an analysis that checks whether agent services are running on the endpoint.

   The following is a sample script for this analysis:

   ```
   Property Name="Threat Mitigation Service Status":
   ```

   ```
   if (exists running service "Threat Mitigation Service")then
   ("Running") else ("Not Running")
   ```

   Relevance:

   ```
   (((if( name of operating system starts with "Win" ) then
   platform id of operating system != 3 else false) AND (name of
   operating system as lowercase starts with "win")) AND (version
   of client >= "5.0")) AND (if (exists key
   "HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" whose
   (exists value "ApplicationPath" of it) of registry) then TRUE
   else FALSE)
   ```

4. If you configured agents to report to Network VirusWall Enforcer servers, in addition to reporting to a Threat Mitigator server, access the TMAgent Manager console, go to the **Server Address** column, and then check if the Network VirusWall Enforcer's IP address is listed.

5. From the TMAgent Manager console, you can also configure agents already reporting to Network VirusWall Enforcer to also report to Threat Mitigator.

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 the TMAgent Manager Console

Agents installed remotely from the TMAgent Manager console can also be uninstalled from the same console. During agent uninstallation, TMAgent Manager client is also uninstalled.

To uninstall the agent from the TMAgent Manager console:

PATH: OFFICESCAN SERVER CONSOLE > PLUG-IN MANAGER > MANAGE PROGRAM > UNINSTALL TMAGENT

1. Select the endpoints from which the agent will be uninstalled.
2. Click **Uninstall TMAgent**. A confirmation message displays.
3. Check the uninstallation status under the **Status** column. After the agent uninstalls, "N/A" displays under the **TMAgent Version** and **Server Address** columns.

Uninstallation from Control Panel

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

Note: When an agent deployed from the TMAgent Manager console is uninstalled directly from Control Panel, TMAgent Manager client is not automatically uninstalled. Uninstall TMAgent Manager client also from the Control Panel.

To uninstall the agent 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 using a 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
```

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

Note: When an agent deployed from the TMAgent Manager console is uninstalled directly using a logon script, TMAgent Manager client is not automatically uninstalled. Uninstall TMAgent Manager client from the Control Panel's Add or Remove Programs screen.

Uninstallation from a Command Line Interface

On the endpoint from which the agent will be uninstalled, open a command prompt, change the directory to `%windir%\PEAgent` and then run the following command:

```
PEAgent.exe /uninstall
```

This command notifies the Threat Management Agent to unregister from Threat Mitigator and then uninstall itself. Check the resulting uninstallation log in:

```
%windir\PEAgent\msiRemoteUninstallTMAgent.log
```

Note: From the Threat Mitigator server, you can also run a command that remotely uninstalls multiple agents. Contact your support provider for details and instructions.

Uninstallation from Trend Micro Endpoint Security Platform

Create a task that silently uninstalls the agent from the endpoint. The script for the task can check whether the following key exists before uninstallation:

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

The following is a sample script for this task:

Relevance:

```
(name of it = "Win2000" OR name of it = "WinXP" OR name of it =
"Win2003" OR (name of it = "WinVista" and product type of it = nt
workstation product type) OR (name of it = "Win2008" or (name of it
= "WinVista" and product type of it != nt workstation product
type))) of operating system AND TRUE AND (if (exists file
"msiexec.exe" of system folder) then true else false) AND  (if
(exists key "HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer"
whose (exists value "ProductCode" of it) of registry) then TRUE else
FALSE)
```

Actions:

```
wait "{pathname of system folder & "\msiexec.exe"}" /x "{(value
"ProductCode" of key
"HKEY_LOCAL_MACHINE\Software\TrendMicro\Policyenforcer" of registry
as string)}" /qn
```

Chapter 5

Performing Threat Mitigation

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

Topics in this chapter:

Note: For an overview of threat mitigation, see *Threat Mitigation* on page 1-3.

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 2-7.

Data Sources

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

- Endpoint security risk logs
- Threat Discovery Appliance

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.

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 Trend Micro Products and Services* on page 1-8.

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 bin 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.

Endpoints excluded from mitigation can be queried from the Threat Management screen but you cannot deploy a custom pattern, run cleanup, or launch On-demand Scan on these endpoints.

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**.
6. To remove an IP address, process, or folder, click the trash bin icon  .

Email Notifications

On the product console's Mitigation Tasks screen, you have the option of running threat mitigation tasks automatically or manually. If you choose to manually perform the tasks, Threat Mitigator can 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.

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 mitigation tasks listed in *Table 5-1* are carried out. For a detailed explanation of these tasks, see *Threat Mitigation* on page 1-3.

TABLE 5-1. Mitigation tasks

TASK	DESCRIPTION
Assessment	Threat Mitigator notifies Threat Management Agent to assess the endpoint after receiving a mitigation request from its data source. Assessment runs automatically.
Post-assessment cleanup	If the assessment confirms the presence of threats in the endpoint, Threat Management Agent runs post-assessment cleanup to eliminate threats. 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 an email reminding you to run cleanup. See step 4 below for details about the email notification.
Threat analysis	If there are unresolved threats after post-assessment cleanup, Threat Management Agent collects forensic data and sends the data to Threat Mitigator. Perform case submission from the Threat Management screen to upload the data to TMSP and have the threats analyzed by a Trend Micro security expert. See *Submit a Case* on page 5-18 for details.

TABLE 5-1. Mitigation tasks (Continued)

TASK	DESCRIPTION
Pattern deployment and custom cleanup	Trend Micro issues either a custom pattern or a new version of smart protection patterns to resolve the remaining threats. After Threat Mitigator downloads the required pattern, it can automatically deploy the pattern to the endpoint or you can manually deploy the pattern from the Threat Management screen. If you choose to manually deploy the pattern, enable email notifications. Threat Mitigator sends an email reminding you to deploy the pattern. See step 4 below for details about the email notification.

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 *Endpoints that require post- assessment cleanup* on page 5-11.
   - **Assess and then automatically run post-assessment 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 7-5.

2. Specify how to deploy the custom pattern downloaded from TMSP, or the Smart Scan Agent Pattern downloaded from the Trend Micro ActiveUpdate server:
   - **Automatically deploy the pattern and run custom cleanup:** Automates the 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 7-5.
   - **Do not run any task:** Allows you to manually deploy the pattern, which you can perform from the Threat Management screen. For details on deploying the pattern, see *Endpoints that require custom cleanup* on page 5-12.

     After the pattern deploys, custom cleanup runs automatically.
3. Select the scan type to use when Threat Management 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. Choose to send an email when:
   - Post-assessment cleanup or pattern deployment should be performed on the Threat Management screen
     - If you choose **Assess the endpoint only** in step 1, Threat Mitigator sends an email after the assessment is complete, notifying you to run post-assessment cleanup.
     - If you choose **Do not run any task** in step 2, Threat Mitigator sends an email after downloading the required pattern, notifying you to deploy the pattern to endpoints.
   - Post-assessment cleanup is unsuccessful

   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 appears after you log on to the Threat Mitigator console (or click **Threat Management** on the left menu bar). In the screen, run security-related tasks that are not configured to run automatically.

Select the target endpoints for each task by using predefined query criteria or by typing the endpoint's IP address or host name.

Predefined Query Criteria

Click the link for each predefined query criteria. Endpoints included in the query result display in the table at the lower section of the screen.

Note: Click the endpoint's IP address under the **IP Address** column to view threat event details for the endpoint.

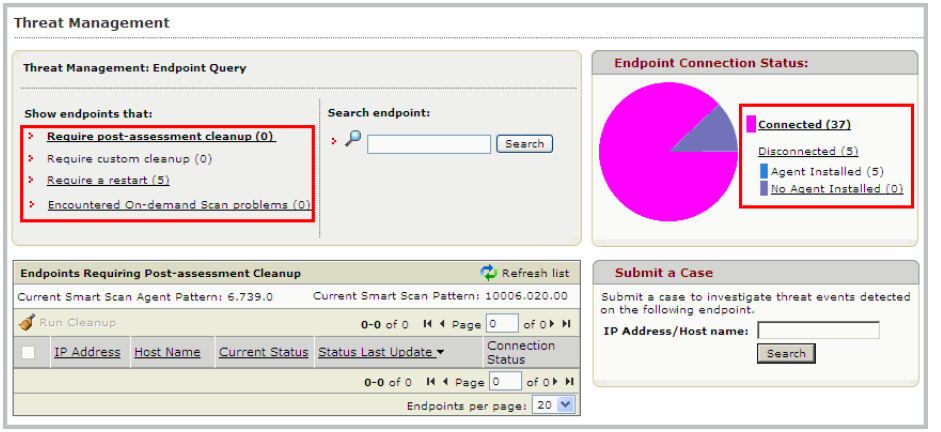


FIGURE 5-1. Threat Management screen with predefined query criteria highlighted

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

TABLE 5-2. Predefined query criteria

QUERY CRITERIA	DESCRIPTION	TASKS
Endpoints that require post-assessment cleanup	Indicates the number of endpoints with security threats that can be eliminated by running post-assessment cleanup The number will always be 0 (zero) if you enabled the option **Assess and then automatically run post-assessment cleanup if required** on the Mitigation Tasks screen.	1. Click **Require post-assessment cleanup**. 2. In the table at the lower section of the screen, select one or more connected endpoints and then click **Run Cleanup**. 3. Check the cleanup result from the Threat Event Logs screen. To open the screen, go to the **IP Address** column in the table and click the IP address.

TABLE 5-2. Predefined query criteria (Continued)

QUERY CRITERIA	DESCRIPTION	TASKS
Endpoints that require custom cleanup	Indicates the number of endpoints that require custom cleanup When there are unresolved threats on an endpoint after running post-assessment cleanup, submit a case to Trend Micro through TMSP. Trend Micro then provides a solution by issuing either a custom pattern or smart protection patterns (Smart Scan Agent Pattern or Smart Scan Pattern, or both). Threat Mitigator downloads the required pattern. The number will always be 0 (zero) if you enabled the option **Automatically deploy the pattern and run custom cleanup** in the Mitigation Tasks screen.	1. Click **Require custom cleanup**. The patterns needed for custom cleanup (either custom pattern or Smart Scan Agent Pattern) display. 2. Click a pattern. Endpoints requiring custom cleanup display in the table at the lower section of the screen. 3. Select one or more connected endpoints and then click **Deploy Pattern**. After the pattern deploys, the endpoint automatically runs custom cleanup. 4. Check the pattern deployment and custom cleanup results from the Threat Event Logs screen. To open the screen, go to the **IP Address** column in the table and click the IP address.

TABLE 5-2. Predefined query criteria (Continued)

QUERY CRITERIA	DESCRIPTION	TASKS
Endpoints that require a restart	Indicates the number of endpoints that need to restart Possible reasons: • The mitigation exception list was updated during threat mitigation. A restart is required to refresh the list and determine if threat mitigation is still required. • Some threats can only be removed completely after a restart. • A Threat Management Agent service will only be loaded after a restart. • Threat Management Agent was updated, but the new version will only become functional after a restart.	1. Click **Require a restart**. 2. In the table at the lower section of the screen, check which endpoints require a restart 3. Instruct endpoint users to restart the endpoint.

TABLE 5-2. Predefined query criteria (Continued)

QUERY CRITERIA	DESCRIPTION	TASKS
Endpoints that encountered On-demand Scan problems	Indicates the number of unsuccessful On-demand Scans launched on the local computer by users. The scan was unsuccessful because one or several infected files were not cleaned.	1. Click **Encountered On-demand Scan problems**. 2. In the table at the lower section of the screen, select one or more connected endpoints, and then click **Launch On-demand Scan** to launch the scan remotely. If this scan encounters issues, Threat Management Agent collects forensic data to be sent to TMSP. 3. For agentless endpoints, instruct users to repeat the scan.
Connected endpoints	Indicates the number of connected endpoints. These endpoints may or may not require mitigation.	Click **Connected**. A list of connected endpoints display in the Endpoint Status screen.
Disconnected endpoints	Indicates the number of disconnected endpoints.	To view all disconnected endpoints, click **Disconnected**. To view only endpoints with agents installed, click **Agent Installed**. To view only agentless endpoints, click **No Agent Installed**. A list of disconnected endpoints display in the Endpoint Status screen.

Endpoints' IP Addresses/Host Names

In the **Search endpoint** text box, type any of the following:

- 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`)
- A complete or partial host name

Note: If you specify a partial host name, the product only returns host names starting with the characters you typed. For example, typing "endpoint" returns "endpoint_001" and "endpoint_002", but does not return "jp_endpoint".

If you type endpoints included in mitigation exceptions, Threat Mitigator will show the endpoints but you cannot deploy a pattern, run custom cleanup, or launch On-demand Scan on these endpoints. For details about mitigation exceptions, see *Mitigation Exceptions* on page 5-5.

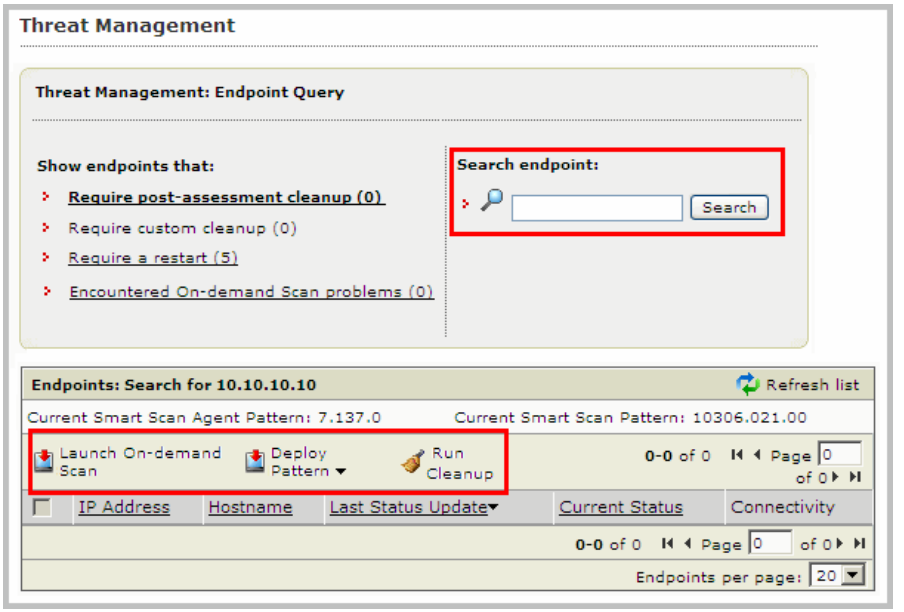


FIGURE 5-2. Threat Management screen with the Search endpoint text box and available tasks highlighted

When the endpoints display on the table, click an endpoint's IP address under the **IP Address** column to view threat event details for the endpoint.

You can run the following tasks on connected endpoints:

- Launch On-demand Scan on the selected or all endpoints. If this scan encountered issues, Threat Management Agent collects forensic data to be uploaded to TMSP. To send forensic data, see *Submit a Case* 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 *Running On-demand Scan* on page 6-6.

- Deploy a pattern to endpoints that require custom cleanup
- Run custom cleanup on endpoints with unresolved threats

Submit a Case

When there are unresolved threats in an endpoint after post-assessment cleanup or administrator-initiated On-demand Scan, Threat Management Agent starts to collect forensic data, which you can send to Trend Micro through TMSP.

If you have TMSP as a hosted service, a Trend Micro security expert will inform you about the unresolved threats, and will ask you perform case submission. The security expert then analyzes the threats and then issues a pattern file through TMSP. If the pattern is a custom pattern created specifically for the unresolved threats, Threat Mitigator automatically downloads the custom pattern.

If you have TMSP as an on-premise application, perform case submission and then log on to TMSP's administrative console to download forensic data. Send the forensic data to Trend Micro for analysis, wait for the pattern file, and then manually upload the pattern to TMSP.

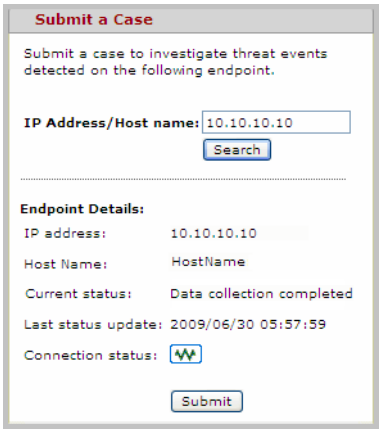


FIGURE 5-3. Threat Management screen - Submit a Case section

Note: Case submission cannot be configured to run automatically.

During case submission:

1. The agent encrypts forensic data and archives it into a .zip file.

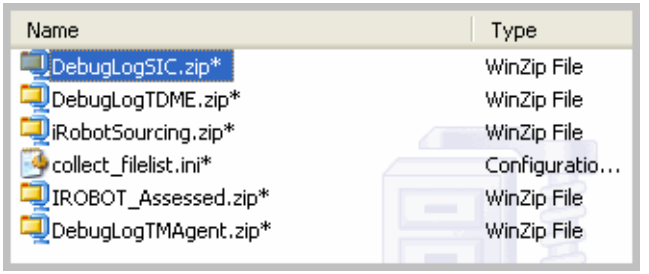


FIGURE 5-4. Sample .zip file containing forensic data

2. The agent uploads the .zip file to Threat Mitigator.
3. Threat Mitigator uploads the .zip file to TMSP.

To perform case submission:

1. Type the endpoint's IP address or host name and click **Search**.
2. Click **Submit**.
3. Check the **Current Status** field. If there are case submission problems, click **Submit** again.

Chapter 6

Running 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 1-7.

This chapter includes the following topics:

On-demand Scan Checklist

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

- *Smart Protection Technology* on page 3-18
- *On-demand Scan Requirements* on page 6-2
- *On-demand Scan Settings* on page 6-4
- *Up-to-Date Components* on page 6-6

On-demand Scan 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	• 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 • Windows 7 (32-bit version)

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

RESOURCES	REQUIREMENTS
Hardware	• 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, 7, or 8
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 Protection Server you have installed, and Internet connection to send scan queries to the Trend Micro Smart Protection Network.

WARNING! On-demand Scan will not start if connection to both the Smart Protection Server and the Trend Micro Smart Protection Network 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 7-5.**

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 acount is used to log on to the computer, a new set of files is downloaded to `<System Drive>/Documents and Settings/<Other User Account>/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, 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 6-6.

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 screen. 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**.

Up-to-Date 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 Protection Technology* on page 3-18.

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.

As an administrator, perform the following tasks to prepare endpoints for On-demand Scan and monitor the scan status:

1. Verify 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

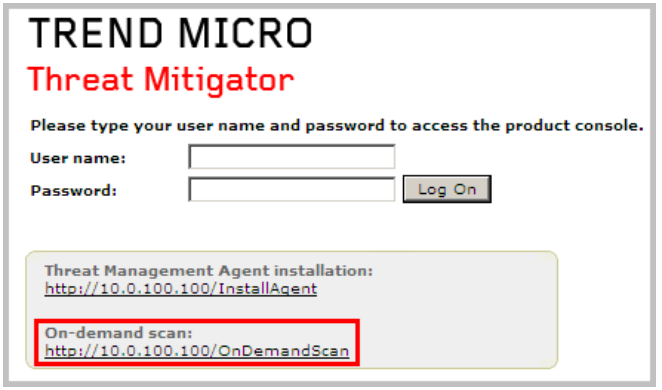


FIGURE 6-1. On-demand Scan link on the Logon screen

   On-demand Scan screen

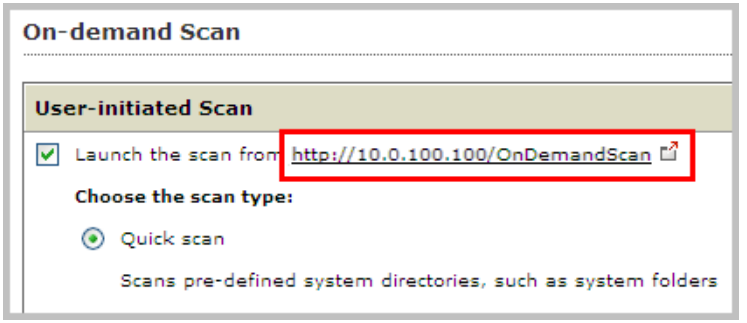


FIGURE 6-2. On-demand Scan link on the On-demand Scan screen

3. Send the On-demand Scan procedure to users who will run On-demand Scan. See *To run On-demand Scan on agentless endpoints:* on page 6-8 for the procedure.
4. 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 7-5 for details). You can instruct users to repeat On-demand Scan to resolve the problems.

To run On-demand Scan on agentless endpoints:

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

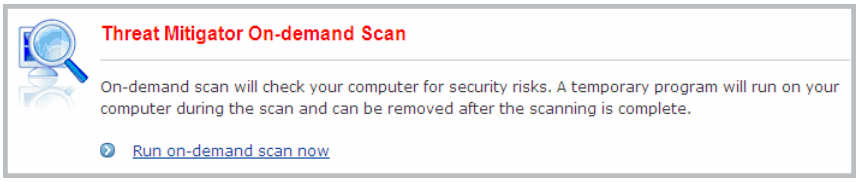


FIGURE 6-3. On-demand Scan start screen

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.

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

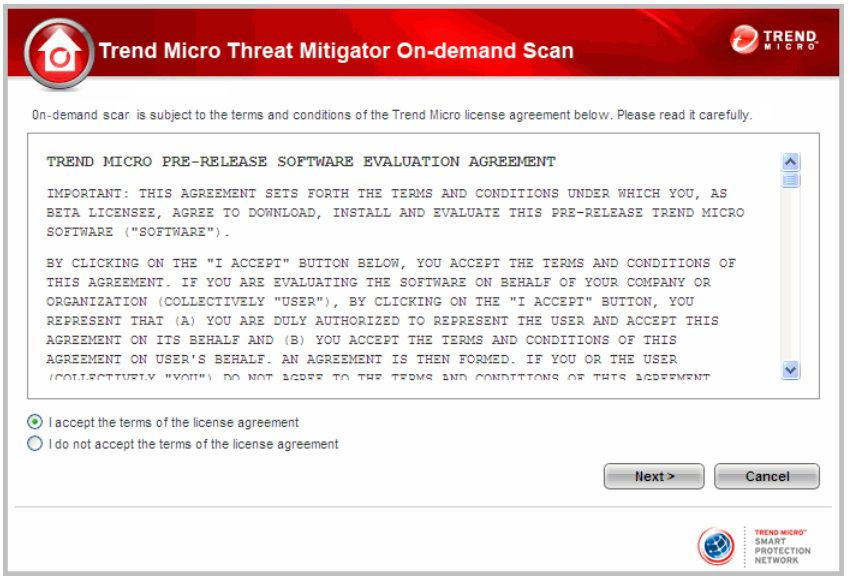


FIGURE 6-4. License agreement screen

5. Click **Scan Now**.

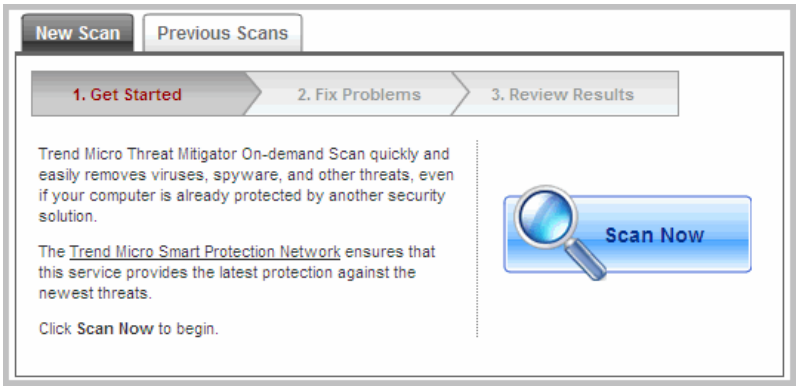


FIGURE 6-5. On-demand Scan main window

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 6-4.

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.

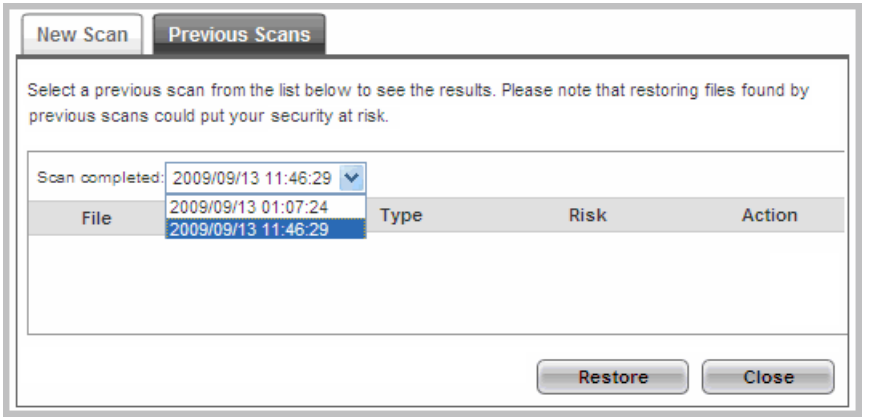


FIGURE 6-6. Previous Scans tab

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 *Running On-demand Scan* on page 6-6.

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 **Connectivity** 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 forensic data. Submit forensic data to Trend Micro by performing case submission. For details, see *Submit a Case* on page 5-18.

Chapter 7

Viewing and Analyzing Information

Regularly monitor endpoints managed by Threat Mitigator by checking their security status and viewing logs. Threat Mitigator keeps comprehensive logs about mitigation events, actions, 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:

Endpoint Status

The following events trigger Threat Management Agent to report the security status of an endpoint to Threat Mitigator:

- An agent sends a heartbeat message to Threat Mitigator. A heartbeat message informs Threat Mitigator that a specific agent is up and running. The interval for sending heartbeat messages is configured in the Agent Settings screen.
- Users run endpoint reassessment by clicking the agent icon in the endpoint's system tray and selecting **Reassess**. After reassessment, the time for sending the next heartbeat message is re-calculated.

Monitor the security status of endpoints from the Endpoint Status screen. In this screen, you can search for:

- All endpoints
- An endpoint by its host name or IP address
- Endpoints with agents connected to Threat Mitigator
- Endpoints with agents disconnected from Threat Mitigator
- Endpoints with outdated agent versions
- Endpoints without Threat Management Agent installed

To query endpoints:

PATH: ENDPOINT STATUS

1. Select a search criteria in **Endpoint status**.
2. If you select **IP address/Host name**, you can type:
   - 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`)
   - A complete or partial host name

   Note: If you specify a partial host name, the product only returns host names starting with the characters you typed. For example, typing "endpoint" returns "endpoint_001" and "endpoint_002", but does not return "jp_endpoint".
3. Click **Search**. Endpoints that meet the search criteria display in the table in the screen.
4. To view endpoint details, click the endpoint's IP address under the **IP Address** column.
5. Check for endpoints with the following status:

TABLE 7-1. Endpoint status that requires attention

COLUMN NAME	STATUS	RECOMMENDED ACTION
Agent Version	An endpoint with **N/A** as its status does not have the agent installed.	Install the agent using the available agent installation methods. Also check the current agent version from the Manual Updates or Scheduled Updates screen. If the agent installed in an endpoint has an older version, upgrade the agent.

TABLE 7-1. Endpoint status that requires attention (Continued)

COLUMN NAME	STATUS	RECOMMENDED ACTION
Connectivity	A green icon  indicates that the endpoint can connect to Threat Mitigator.	None
Connectivity	A red icon  indicates that the endpoint is disconnected from Threat Mitigator and therefore cannot run mitigation tasks. For details, see *Disconnected Endpoints* on page A-2.	Verify the connection by clicking the icon. The icon turns green if connection was restored.

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 during mitigation

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 **More search criteria** to refine the query scope. Select from the following criteria:

TABLE 7-2. Additional search criteria

SEARCH CRITERIA	DESCRIPTION
IP address range	A range of IP addresses for endpoints
Host name	The endpoint's host name **Note:** Host names may not display properly due to encoding language conflicts, which can be resolved by configuring host name encoding in the Log Settings screen. For details, see *Log Settings* on page 7-21.

TABLE 7-2. Additional search criteria (Continued)

SEARCH CRITERIA	DESCRIPTION
Threat event	Includes the following threat-related events logged by Threat Mitigator or Threat Management Agent: • **Threat detection (from security risk logs):** A threat was detected after analyzing logs from endpoint security software such as OfficeScan • **User-initiated On-demand Scan:** A user launched On-demand Scan on an agentless endpoint • **Agent post-installation scan:** The endpoint was scanned immediately after the agent was installed • **Custom pattern <x> deployment:** The specified custom pattern was deployed to an endpoint • **Administrator-initiated On-demand Scan:** You launched On-demand Scan remotely from the Threat Management screen • **Post-assessment cleanup:** The agent assessed the endpoint for threats and then performed cleanup • **Forensic data collection:** The agent collected forensic data from the endpoint because there are unresolved threats after post-assessment cleanup **Note:** Threat-related events not listed in this document but are appearing in the web console are events that Threat Discovery Appliance reports to Threat Mitigator.

TABLE 7-2. Additional search criteria (Continued)

SEARCH CRITERIA	DESCRIPTION
Data source	Entities or tasks that generate threat event information, including: • Threat Discovery Appliance • Threat Management Services Portal • Security risk logs • Cleanup using custom pattern • On-demand Scan (user-initiated, with agent) • On-demand Scan (user-initiated, agentless) • On-demand Scan (administrator-initiated) • Agent post-installation scan

TABLE 7-2. Additional search criteria (Continued)

SEARCH CRITERIA	DESCRIPTION
Mitigation status	Threat events grouped by the following status groups: • **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. • **Unsuccessful:** The mitigation task was not completed or encountered problems. • **Resolved threats:** All or selected threats have been resolved. • **Assessed endpoint:** The agent detected threats in the endpoint during assessment but did not run cleanup because you have chosen to run cleanup manually. • **Rollback successful:** A mitigation task was rolled back successfully. • **Rollback unsuccessful:** A mitigation task was not rolled back. • **Scanned endpoint:** On-demand Scan has been completed. Either no threat was found or the user chose to ignore all detected threats. **Note:** For mitigation status details, see *Mitigation Status* on page 7-9.

3. Click **Search**. A **Query Result** table appears.
4. To view threat event details, click a link under the **Mitigation Status** column. For details, see *Mitigation Status* on page 7-9.
5. To undo mitigation tasks, select one or several endpoints and then click **Rollback**.
6. To export the query results, click **Export to CSV**.

Mitigation Status

The Threat Event Logs screen in the console displays the status for the following tasks:

- Threat mitigation
- On-demand Scan (user-initiated and administrator-initiated)
- Agent post-installation scan

This topic discusses Trend Micro recommended actions when tasks are not successfully carried out.

TABLE 7-3. Task status

STATUS	TASK	DESCRIPTION AND RECOMMENDED ACTIONS
STATUSES THAT DO NOT REQUIRE ANY ACTION		
Mitigation in progress	• Threat mitigation • Administrator-initiated On-demand Scan • Post-installation scan	Threat Mitigator received an event from a data source and is waiting for the agent to process the mitigation task.

TABLE 7-3. Task status (Continued)

STATUS	TASK	DESCRIPTION AND RECOMMENDED ACTIONS
Resolved threats: All threats resolved	• Threat mitigation • Administrator-initiated On-demand Scan • User-initiated On-demand Scan • Post-installation scan	The agent has resolved all threats detected on the endpoint.
Resolved threats: Endpoint security software took action	Threat mitigation	Endpoint security software (such as OfficeScan) took a specific action on the infected file before the agent can take action. For a list of actions the security software can perform, refer to the documentation for the software.
Resolved threats: Threat no longer exists	Threat mitigation	A threat reported by the data source no longer exists at the time of cleanup. The threat may have been removed from the endpoint.
Resolved threats: Potential threat resolved	Threat mitigation	An item that has the potential of becoming a threat was confirmed as safe during cleanup.
Scanned endpoint: No threat found	• Administrator-initiated On-demand Scan • User-initiated On-demand Scan • Post-installation scan	No threats were found on the endpoint. **Note:** The number of files scanned during the scan depends on the scan type. For details about scan types, see *To configure On-demand Scan settings:* on page 6-4.

TABLE 7-3. Task status (Continued)

STATUS	TASK	DESCRIPTION AND RECOMMENDED ACTIONS
Rollback successful	• Threat mitigation • Administrator-initiated On-demand Scan • Post-installation scan	The agent successfully rolled back the mitigation action.
STATUSES THAT REQUIRE AN ACTION		
Assessed endpoint: Manual cleanup needed	Threat mitigation	The agent detected threats in the endpoint during assessment but did not run cleanup because you have chosen to run cleanup manually. 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 **Run Cleanup**.

TABLE 7-3. Task status (Continued)

STATUS	TASK	DESCRIPTION AND RECOMMENDED ACTIONS
No mitigation: Mitigation exception	• Threat mitigation • Administrator-initiated On-demand Scan • Post-installation scan	The agent cannot perform the task because of a mitigation exception. For example, the endpoint's IP address might be included in the mitigation exception list. 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. **Note:** Threat Discovery Appliance also has its own exception list. Threat Discovery Appliance monitors endpoints included in its exception list but does not send mitigation requests to Threat Mitigator.
Resolved threats: All selected threats resolved	User-initiated On-demand Scan	Threats that the user chose to resolve have been resolved. The user chose to leave other threats unresolved. Check if there is a reason for not resolving the remaining threats (for example, the infected 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.

TABLE 7-3. Task status (Continued)

STATUS	TASK	DESCRIPTION AND RECOMMENDED ACTIONS
Scanned endpoint: No action performed on threats	User-initiated On-demand Scan	Users can manually select the threats to resolve. The user chose to leave all the detected threats unresolved. Check if there is a reason for not resolving the threats (for example, the infected 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: Mitigation timeout	Threat mitigation	The agent did not finish a task within a certain time period. Actions: 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 7-3. Task status (Continued)

STATUS	TASK	DESCRIPTION AND RECOMMENDED ACTIONS
Unsuccessful: Cannot connect to endpoint	• Threat mitigation • Administrator-initiated On-demand Scan • Post-installation scan	Threat Mitigator notified the agent to run a task. However, the agent was unreachable. **Note:** The agent is considered unreachable if unresponsive within 3 hours. Verify the following: • The endpoint runs a supported operating system. For details, see *Agent Requirements* on page 4-3. • The agent is installed and is currently up and running. • The endpoint 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	• Threat mitigation • Administrator-initiated On-demand Scan • Post-installation scan	The agent is running and can run mitigation tasks but the endpoint's operating system does not support the mitigation task. If the endpoint's operating system supports On-demand Scan: • Try launching the scan from the Threat Management screen. • Instruct the user to run the scan directly on the endpoint. For details about launching or running On-demand Scan, see *Running On-demand Scan* on page 6-6.

TABLE 7-3. Task status (Continued)

STATUS	TASK	DESCRIPTION AND RECOMMENDED ACTIONS
Unsuccessful: Incomplete task	• Threat mitigation • Administrator-initiated On-demand Scan • Post-installation scan	There were pending tasks before a deliberate or unexpected restart of Threat Mitigator. Upon restart, Threat Mitigator was unable to resume the tasks. Collect system logs and then send them to your support provider.
Unsuccessful: Not all threats resolved	• Threat mitigation • Administrator-initiated On-demand Scan • User-initiated On-demand Scan • Post-installation scan	The agent was unable to resolve all threats. Actions: • Review the threats listed in the **Clean History** tab in the Event Details screen. You can manually remove detected threats that you consider harmless. • Ask the user to run On-demand Scan again to resolve the threats. • If the threats cannot be resolved, 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. Task status (Continued)

STATUS	TASK	DESCRIPTION AND RECOMMENDED ACTIONS
Unsuccessful: Not all selected threats resolved	User-initiated On-demand Scan	Some of the threats that the user chose to resolve were not resolved possibly because of errors in the On-demand Scan program or the agent. The user also chose to leave other threats unresolved. Actions: 1. Ask the user to run On-demand Scan again to resolve the threats. 2. If the threats cannot be resolved, 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 resolving the threats the user chose not to resolve (for example, the infected 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: Agent component problem	Threat mitigation	Components used by the agent will only be functional when the endpoint restarts. Restart the endpoint.

TABLE 7-3. Task status (Continued)

STATUS	TASK	DESCRIPTION AND RECOMMENDED ACTIONS
Unsuccessful: Agent component error	• Threat mitigation • Administrator-initiated On-demand Scan • User-initiated On-demand Scan • Post-installation scan	The agent cannot perform the task because a component used by the agent encountered an error. Actions: 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.
Unsuccessful: Corrupted configuration file	• Threat mitigation • Administrator-initiated On-demand Scan • User-initiated On-demand Scan • Post-installation scan	A configuration file required to run a task is corrupted. Actions: 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.
Unsuccessful: Pattern not found	• Threat mitigation • Administrator-initiated On-demand Scan • Post-installation scan	A custom pattern required to run a task is not available. On the Threat Management screen, check the custom patterns currently available on Threat Mitigator. If the pattern does not exist and you have TMSP as an on-premise application, try to deploy the pattern from TMSP's administrative console. If you have TMSP as a hosted service, contact your Trend Micro representative for help.

TABLE 7-3. Task status (Continued)

STATUS	TASK	DESCRIPTION AND RECOMMENDED ACTIONS
Unsuccessful: Cannot send scan query	• Threat mitigation • Administrator-initiated On-demand Scan • User-initiated On-demand Scan • Post-installation scan	The agent cannot start a task because it cannot send scan queries to the Smart Protection Server or the Trend Micro Smart Protection Network. If the task has started and the endpoint loses connection with Smart Protection Server and Smart Protection Network, it bypasses files requiring a scan query. Users can proceed to access the files. Ensure that smart protection settings are correct and that there is a functional connection between the endpoint and Smart Protection Server or Smart Protection Network. For details, see *Smart Protection Technology* on page 3-18.

TABLE 7-3. Task status (Continued)

STATUS	TASK	DESCRIPTION AND RECOMMENDED ACTIONS
Rollback unsuccessful	• Threat mitigation • Administrator-initiated On-demand Scan • Post-installation scan	The agent was unable to completely roll back files, registry keys, or services because the backup file does not exist or is corrupted. To complete the roll back: 1. Locate the Task ID for the mitigation task from the Event Details screen. 2. Navigate to `C:\%WINDIR%\PEAgent\iRobot\log\` and check if the `%TaskID%` folder exists. 3. On the `%WINDIR%\PEAgent\iRobot` folder, type the following command: `HouseCallCLI.exe -RE -SID=%TaskID%` **Note:** Navigate to the Event Details screen of each task to locate `TaskID`. 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.

System Logs

Threat Mitigator creates a log entry when the system updates, restarts, or performs other 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 Settings

The Log Settings screen allows you to perform the following tasks:

- Specify the host name encoding language.

  Threat Mitigator's encoding language is UTF-8. An endpoint's host name may not display properly in Threat Event Logs if the host name information retrieved from the endpoint is encoded in another language. To display the information properly, Threat Mitigator must first determine the original encoding language and then convert the host name from that language to UTF-8.

  Threat Mitigator can convert the host name from any of the encoding languages provided in the **Host Name Encoding** section.
- Specify syslog servers to which Threat Mitigator sends threat event logs and system logs.

To configure log settings:

PATH: LOGS > LOG SETTINGS

1. Select the encoding language from the list.
2. Select the check box to send logs to the primary syslog server.
3. Type the IP address and port number of the primary syslog server.
4. (Optional) Select the check box to send logs to the secondary syslog server to manage logs on a backup or duplicate syslog application.
5. Type the IP address and port number of the secondary syslog server.
6. 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

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 > SYSTEM 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.

You can add up to 50 administrative accounts.

To configure administrative accounts:

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.
6. To remove an account, select it and then click **Delete**. You can remove the default Power User and Operator accounts, but not the default Administrator account.

Access Control

Configure Access Control settings to regulate access to the Threat Mitigator web-based and preconfiguration consoles.

To configure Access Control settings:

PATH: ADMINISTRATION > SYSTEM CONFIGURATION > ACCESS CONTROL

1. Select the option to allow SSH connections to the preconfiguration console.

   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: • 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: • **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 and Queries

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

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 and Queries

OBJECT NAME	OBJECT IDENTIFIER (OID)	DESCRIPTION
coldStart	.1.3.6.1.6.3.1.1.5.1	Signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered
Shutdown	.1.3.6.1.4.1.8072.4.0.2	Signifies that Threat Mitigator was shut down
ProductVersion	.1.3.6.1.4.1.6101.3001.1.0	Returns the Threat Mitigator version
RequiringPost Assessment Cleanup	.1.3.6.1.4.1.6101.3001.2.1.0	Returns the number of endpoints requiring post-assessment cleanup, as indicated on the Threat Management screen
RequiringCustom Solution	.1.3.6.1.4.1.6101.3001.2.2.0	Returns the number of endpoints requiring custom cleanup, as indicated on the Threat Management screen

TABLE 8-3. SNMP Traps and Queries (Continued)

OBJECT NAME	OBJECT IDENTIFIER (OID)	DESCRIPTION
OnDemandScan Fail	.1.3.6.1.4.1. 6101.3001.2.3. 0	Returns the number of endpoints that encountered On-demand Scan problems, as indicated on the Threat Management screen
bootFactory	.1.3.6.1.4.1. 6101.3001.3.4	Threat Mitigator booted to the default factory partition.
bootPrevious	.1.3.6.1.4.1. 6101.3001.3.5	Threat Mitigator booted to the previous partition.
databaseMainten ance	.1.3.6.1.4.1. 6101.3001.3.7	The database shrink process was carried out to reduce the size of the database.
logPurge	.1.3.6.1.4.1. 6101.3001.3.8	Database logs were purged. This object references "logPurgeType" to check whether purging was done manually or automatically.
connectTMSPFail	.1.3.6.1.4.1. 6101.3001.3.9	Threat Mitigator was unable to connect to TMSP. Threat Mitigator establishes connections at 10-minute intervals. This object references "serverLocation" to determine the IP address or host name of TMSP.
NTPFail	.1.3.6.1.4.1. 6101.3001.3.10	Threat Mitigator was unable to synchronize its system time with the NTP server.

TABLE 8-3. SNMP Traps and Queries (Continued)

OBJECT NAME	OBJECT IDENTIFIER (OID)	DESCRIPTION
customSolution Downloaded	.1.3.6.1.4.1. 6101.3001.3.11	A pattern required for custom cleanup is ready for deployment to affected endpoints. This object references the following objects: • **solutionType:** Type of pattern required for custom cleanup (Custom pattern or Smart Scan Agent Pattern) • **solutionVersion:** Version of the custom pattern required for custom cleanup • **endpointList:** List of endpoints requiring custom cleanup
connectAUFail	.1.3.6.1.4.1. 6101.3001.3.12	An attempt to connect to the Trend Micro ActiveUpdate server was unsuccessful.
component UpdateFail	.1.3.6.1.4.1. 6101.999.2.2	Connection with the Trend Micro ActiveUpdate was established but the update session was unsuccessful. Each session updates one or several components. The component names are listed, but version numbers are not.

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 and view its content:
    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.

Threat Mitigator, Smart Protection Server, and the VMware ESX/ESXi server (which hosts the Smart Protection Server and Threat Mitigator) require unique IP addresses. Check the IP addresses of the VMware ESX/ESXi server and Smart Protection 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 2-7.

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**.

Note: Enabling **Separate Management Interface** in the IP Address Settings screen binds the **Bound To** port to the management interface. Disabling the option binds the port to the data interface.

---

3. Click **Save**.
4. To delete a static route, select it and then click **Delete**.

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.**

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 start using these tools.

TABLE 8-4. Support tools

TOOL	DESCRIPTION
System Information Collector (SIC) Tool	SIC gathers detailed computer configuration that helps isolate and identify known or potential threats in an endpoint. For details on how to obtain and use this tool, visit the following page: http://www.trendmicro.com/download/sic.asp Updates to this tool can be uploaded to Threat Mitigator through the product console's Support Tools screen.
Case Diagnostic Information	Case Diagnostic Information downloads information required for use with the Case Diagnostic Tool. The tool is used for debug purposes.
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 system 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 system 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 system 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 website:** 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\
  ```

Chapter 9

Troubleshooting and Support

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

This chapter contains the following topics:

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. For more information about this tool, see *Support Tools* on page 8-14.

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\*.*`
  - `%WINDIR%\PEAgent\iRobot\log\*.*`

Threat Mitigator Debug Information

Collect the debug logs using the Case Diagnostic Tool. For details, see *Case Diagnostic Information* on page 8-14.

Troubleshooting

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

System 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 Threat Mitigator and Network VirusWall Enforcer 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.

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%\apppatch\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.

Before Contacting Technical Support

Before contacting technical support, please consider visiting the following Trend Micro online resources.

Trend Community

Get help, share your experiences, ask questions, and discuss security concerns in the forums with fellow users, enthusiasts, and security experts.

http://community.trendmicro.com/

The Trend Micro Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro website, 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 website.

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

Contacting Trend Micro

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.

- Get a list of the worldwide support offices at:

  http://www.trendmicro.com/support

- Get the latest Trend Micro product documentation at:

  http://downloadcenter.trendmicro.com/

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

When you contact Trend Micro, to speed up your problem resolution, ensure that you have the following details available:

- Microsoft Windows and Service Pack versions
- Network type
- Computer brand, model, and any additional hardware connected to your computer
- Amount of memory and free hard disk space on your computer
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

TrendLabs

TrendLabs[SM] 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 website 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

Appendix A

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 **Connectivity** column indicates that the endpoint is agentless.

Note: A red-colored icon also displays if the endpoint is disconnected.

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  under the **Connectivity** column indicates that the agent is connected.

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 3-22.

Disconnected Endpoints

Disconnected endpoints include:

- Endpoints with agents reporting to Threat Mitigator. If these endpoints require mitigation, mitigation tasks will only run when connection to Threat Mitigator is established.

  An agent is considered "disconnected" if it was unable 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 3-22.
- Endpoints with agents that Threat Mitigator used to managed. The agents are now reporting to other Threat Mitigator servers.
- Agentless Endpoints that have run On-demand Scan.

On the Threat Management screen, a red-colored icon  under the **Connectivity** column indicates that the endpoint is disconnected.

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

Q

R

S

T

U

V

W