TREND MICRO

Threat Discovery Appliance 2.6

Administrator's Guide

TREND MICRO SMART PROTECTION NETWORK

Endpoint Security

Network Security

Protected Cloud

Release Date: August 2010

Document Part No: APEM24566/100810

Protected by U. S. Patent No. 7,516,130

The Administrator's Guide for Trend Micro™ Threat Discovery Appliance is intended to introduce the main features of the product, provide deployment information for your production environment, and provide information on configuring and using the product. Read through this document prior to deploying or using the product.

Detailed information about how to use specific features are available in the online help file and the online Knowledge Base at Trend Micro's website.

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

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

Contents

Chapter 3: Installing Threat Discovery Appliance

Chapter 4: The Preconfiguration Console

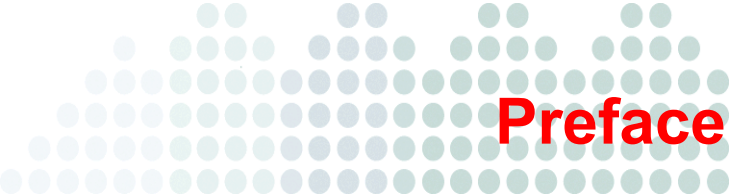
Chapter 5: Getting Started

Chapter 6: Configuring Product Settings

Chapter 7: Viewing and Analyzing Information

Chapter 8: Maintenance

Chapter 9: Getting Help



Preface

Welcome to the Administrator' Guide for Trend Micro™ Threat Discovery Appliance. This manual contains information about product setup and configuration.

This preface discusses the following topics:

Terminology and Documentation

The following terminology is used throughout the documentation:

TABLE P-1. Terminology used in the product documentation

TERMINOLOGY	DESCRIPTION
appliance	Threat Discovery Appliance in device form. This product form factor is not available in this release.
virtual appliance	Threat Discovery Appliance as a virtual application installed on a VMware server; its full name is Threat Discovery Virtual Appliance. This product form factor is also not available in this release.
software appliance	Threat Discovery Appliance as software installed on a bare metal server or a virtual machine. This is the only form factor available in this release. Unless otherwise indicated, all instances of the product name ("Threat Discovery Appliance" or "product") refer to the software appliance.

The product documentation consists of the following:

TABLE P-2. Product documentation

DOCUMENTATION	DESCRIPTION
Administrator's Guide	A PDF document that discusses product setup and configuration
Help	HTML files compiled in WebHelp format that provide "how to's", usage advice, and field-specific information. To access the Help, open the product console and then click the help icon. 

TABLE P-2. Product documentation (Continued)

DOCUMENTATION	DESCRIPTION
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 Discovery Appliance 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 and readme file are available in the Threat Discovery Appliance Solutions CD and at the following website:

http://downloadcenter.trendmicro.com/

Audience

The Threat Discovery Appliance documentation is written for IT managers and 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, the Threat Discovery Appliance documentation uses the following conventions.

TABLE P-3. 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
LOGS > LOG MAINTENANCE	A "breadcrumb" found at the start of procedures that helps users navigate to the relevant web console screen. Multiple breadcrumbs means that there are several ways to get to the same screen.
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 Discovery Appliance

This chapter introduces product features, capabilities, and technology.

The topics discussed in this chapter are:

About Threat Discovery Appliance

Threat Discovery Appliance is a next-generation network monitoring product that uses a combination of intelligent rules, algorithms, and signatures to detect a variety of malware including worms, Trojans, backdoor programs, viruses, spyware, adware, and other threats. Detection is done at layers 2 to 7 of the Open Systems Interconnection Reference Model (OSI model).

Threat Discovery Appliance delivers high-performance throughput and availability and provides IT administrators with critical security information, alerts, and reports.

Deploy Threat Discovery Appliance as a standalone product or as part of Threat Management Services, a threat lifecycle management suite that includes Threat Mitigator and Threat Management Services Portal (TMSP). For details, see *About Trend Micro Threat Management Services* on page 1-2.

Note: For a complete list of Trend Micro products and services that integrate with Threat Discovery Appliance, see *Integration with Trend Micro Products and Services* on page 6-19.

About Trend Micro 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 Smart Protection Network™ to identify and respond to next-generation threats.

For an overview of the solutions provided by Threat Management Services and how these solutions work together, refer to the Threat Management Services Deployment Guide.

Product Form Factor

In this product release, Threat Discovery Appliance is available as a software appliance that can be installed on a bare metal server or a VMware virtual machine. For some customers, the software appliance may come pre-installed on a server-class device.

The appliance and virtual appliance are not available in this release. Users who have set up the appliance or virtual appliance can upgrade to this product version by performing a fresh installation of the software appliance. Back up configuration and other settings before installation, and then restore them after installation.

To perform a fresh installation of the software appliance, follow the steps outlined in *Installing Threat Discovery Appliance* on page 3-4.

New in This Release

This product release introduces the following new features and enhancements:

TABLE 1-1. New in Threat Discovery Appliance 2.6

WHAT'S NEW	DESCRIPTION
Integration with Trend Micro smart protection technology	Threat Discovery Appliance now leverages Trend Micro smart protection technology to check the reputation of websites that users are accessing. Threat Discovery Appliance logs URLs that smart protection technology verifies to be fraudulent or known sources of threats. The product uploads the logs to TMSP for report generation. For details, see *Smart Protection Technology* on page 6-21.
System updates	Threat Discovery Appliance makes use of system updates to address issues, enhance product performance, or even adopt new features. A rollback function is provided to undo the changes applied by system updates. For more information, see *System Updates* on page 8-6.
Real-time notifications	Receive notifications immediately or at specified intervals when Threat Discovery Appliance detects critical security risks. For more information, see *Real-time Notification for Critical Security Risks* on page 7-16.
Web console timeout	Configure how long Threat Discovery Appliance waits before logging out an inactive web console user session. For more information, see *Web Console Timeout* on page 8-2.

TABLE 1-1. New in Threat Discovery Appliance 2.6 (Continued)

WHAT'S NEW	DESCRIPTION
Monitoring of private networks	Threat Discovery Appliance now automatically configures IP address blocks reserved by the Internet Assigned Numbers Authority (IANA) for private networks in its monitored network. For details about monitored networks, see *Monitored Networks* on page 6-2.

Features and Benefits

Threat Discovery Appliance uses the mirror port of the switch to monitor network traffic and detect known and potential security risks. Threat Discovery Appliance provides the following features and benefits:

Virus Scan Engine

The Virus Scan Engine is a file-based detection-scanning engine that has true file type, multi-packed files, and IntelliTrap detection. The scan engine performs the actual scanning across the network and uses the virus pattern file to analyze the files traveling throughout your network. The virus pattern file contains binary patterns of known viruses. Trend Micro regularly releases new virus pattern files when new threats arise. To take advantage of the latest components, regularly update Threat Discovery Appliance (see *Component Updates* on page 5-12).

The virus scan engine has the following methods of detection:

- True File Type
- Multi-packed/Multi-layered files
- IntelliTrap

True File Type

Virus writers can quickly rename files to disguise the file's actual type. Threat Discovery Appliance confirms a file's true type by reading the file header and checking the file's internally registered data type. Threat Discovery Appliance only scans file types capable of infection.

With true file type, Threat Discovery Appliance determines a file's true type and skips inert file types. Inert file types include files such as `.gif` files, which make up a large volume of Internet traffic.

Multi-packed/Multi-layered Files

A multi-packed file is an executable file compressed using more than one packer or compression tool. For example, an executable file double or triple packed with Aspack, UPX, then with Aspack again.

A multi-layered file is an executable file placed in several containers or layers. A layer consists of a document, an archive, or a combination of both. An example of a multi-layered file is an executable file compressed using Zip compression and placed inside a document.

These methods hide malicious content by burying them under multiple layers of compression. Traditional antivirus programs cannot detect these threats because traditional antivirus programs do not support layered/compressed/packed file scanning.

IntelliTrap

Virus writers often use different file compression schemes to circumvent virus filtering. IntelliTrap helps Threat Discovery Appliance evaluate compressed files that could contain viruses or other Internet threats.

Network Virus Scan

Threat Discovery Appliance uses a combination of patterns and heuristics to proactively detect network viruses. The product monitors network packets and triggers events that can indicate an attack against a network. The product can also scan traffic in specific network segments.

Network Content Inspection Engine

Network Content Inspection Engine is the program module used by Threat Discovery Appliance that scans the content that passes through the network layer.

Network Content Correlation Engine

Network Content Correlation Engine is the program module used by Threat Discovery Appliance that implements rules or policies defined by Trend Micro. Trend Micro regularly updates these rules after analyzing the patterns and trends that new and modified viruses exhibit.

Potential Risk File Capture

A potential risk file is a file the Network Content Inspection Engine categorizes as potentially malicious. However, the Virus Scan Engine does not recognize known signature patterns of verified malicious files and does not categorize the file as malicious or as a security risk. Threat Discovery Appliance captures potential risk files, enters a log in the database, and saves a copy of the file. Threat Discovery Appliance captures the file session and threat information as a file header and stores data in the log file.

Offline Monitoring

Threat Discovery Appliance deploys in offline mode. It monitors the network traffic by connecting to the mirror port on a switch for minimal or no network interruption.

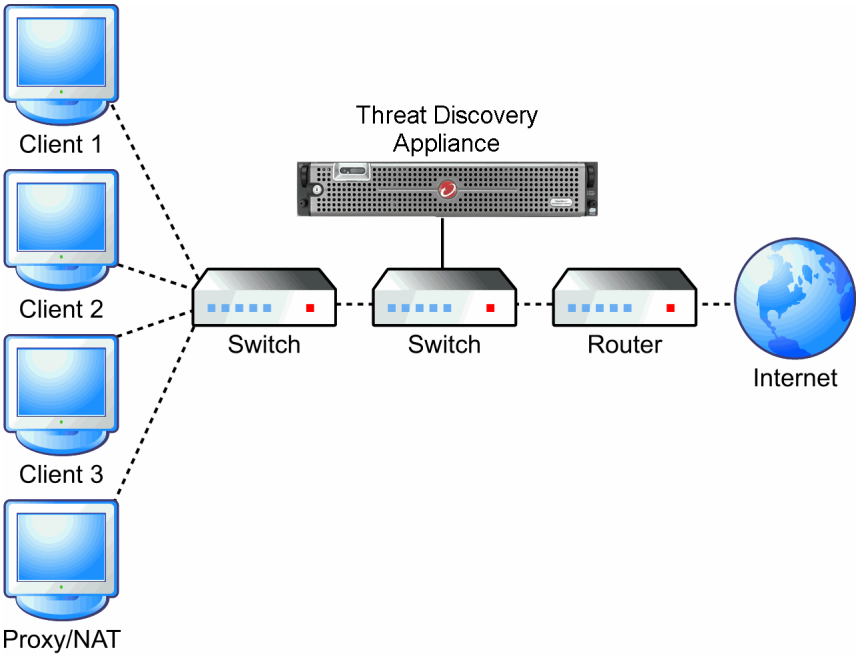


FIGURE 1-1. Product deployment

Multiple Protocol Support

Threat Discovery Appliance monitors network activities that use the HTTP, FTP, SMTP, SNMP, and P2P protocols.

Chapter 2

Deploying Threat Discovery Appliance

This chapter provides tips, suggestions, and requirements for deploying Threat Discovery Appliance.

The topics discussed in this chapter are:

Deployment Considerations

Consider the following before deploying Threat Discovery Appliance to your network.

- Port speeds must match

  The destination port speed should be the same as the source port speed to ensure equal port mirroring. For example, if the destination port is unable to cope with the information due to the faster speed of the source port, the destination port might drop some data.

- The product monitors the complete data flow

  Ensure that Threat Discovery Appliance monitors the complete data flow. This means that Threat Discovery Appliance should monitor all the data coming to and from the network.

Deployment Scenarios

Use the following examples to help you plan Threat Discovery Appliance deployment.

Single Port

In this scenario, connect the Threat Discovery Appliance data port to the mirror port of the core switch, which mirrors the port to the firewall.

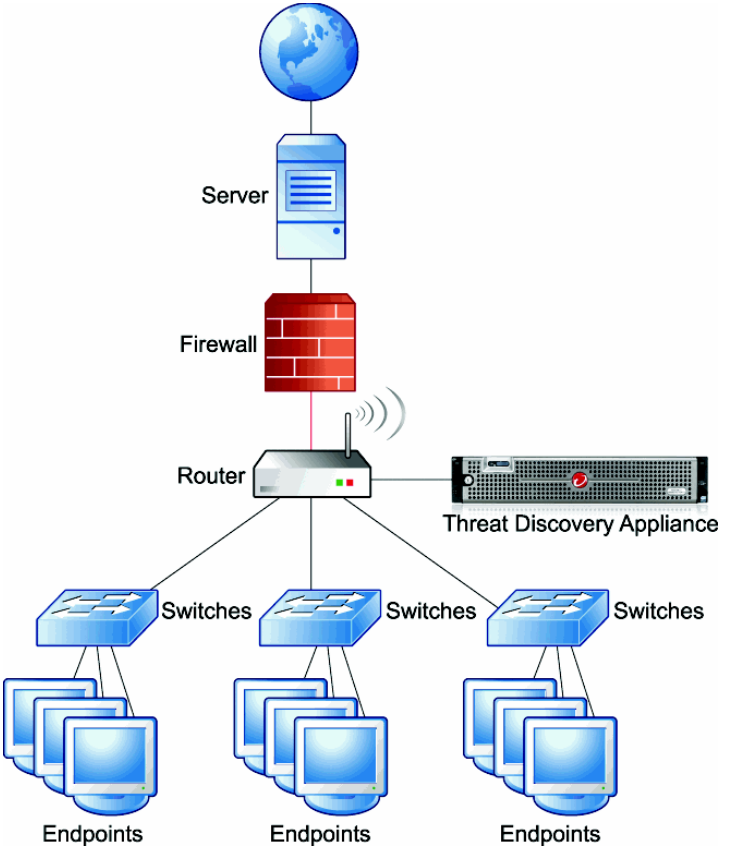


FIGURE 2-2. Single port monitoring

Dual Port

Threat Discovery Appliance can monitor different network segments using its different data ports. In this scenario, connect Threat Discovery Appliance data ports to the mirror ports of access or distribution switches.

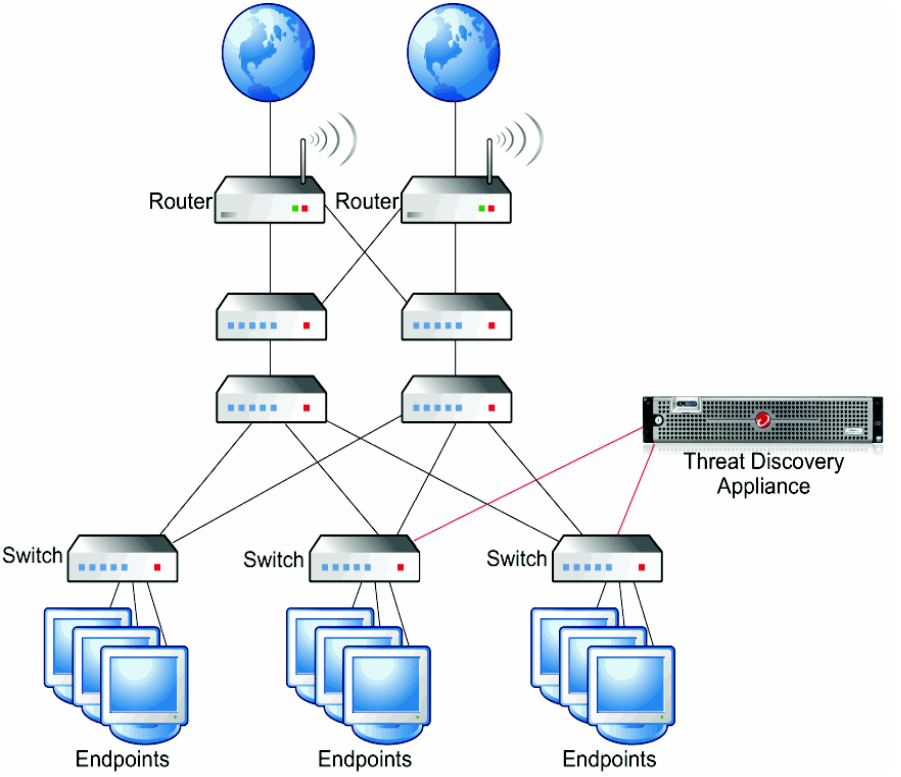


FIGURE 2-3. Dual port monitoring

Network TAP

Network TAPs can monitor the data flowing across the network from interconnected switches, routers, and computers. In this scenario, connect Threat Discovery Appliance to a network TAP.

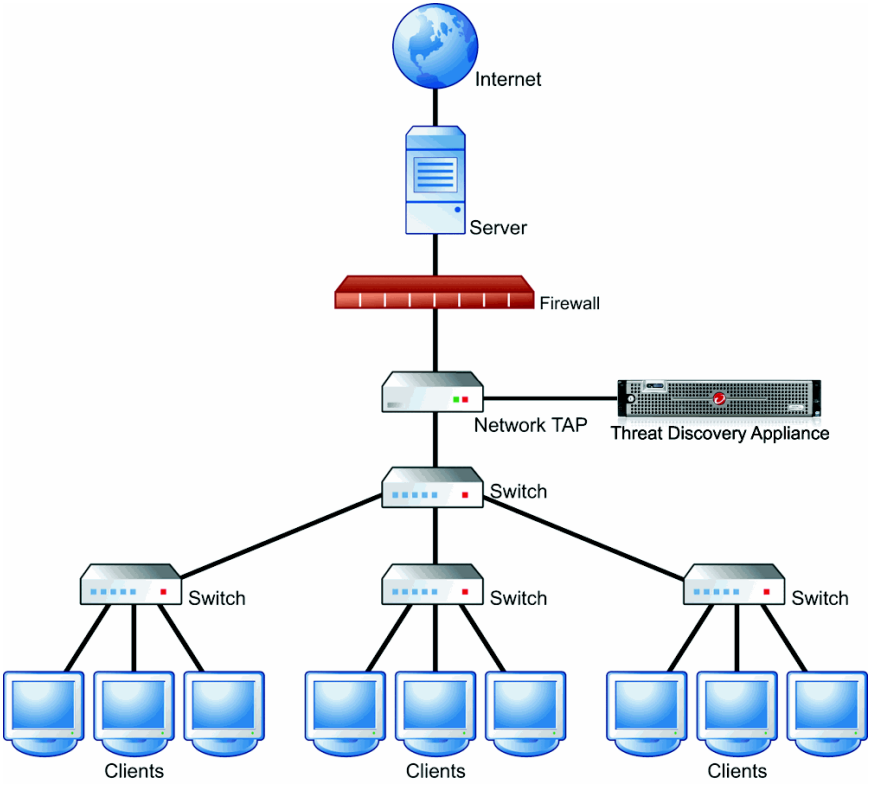


FIGURE 2-4. Single Threat Discovery Appliance connected to a network TAP

Additionally, use an Intrusion Detection System load balancer for better performance when deploying several instances of Threat Discovery Appliance.

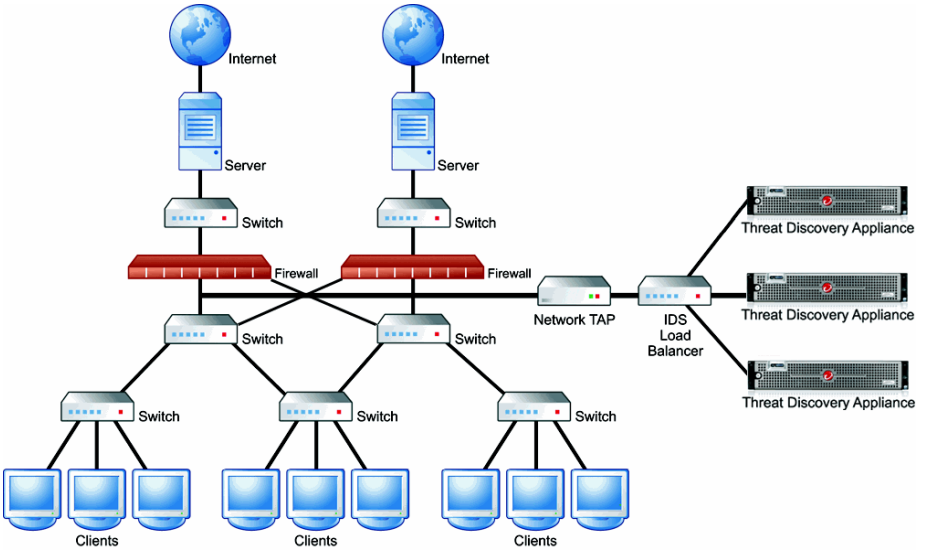


FIGURE 2-5. Several Threat Discovery Appliances connected to a network TAP

Redundant Networks

Most enterprise environments use redundant networks to provide high availability. In these scenarios where asymmetric route is possible, connect Threat Discovery Appliance to the redundant switches.

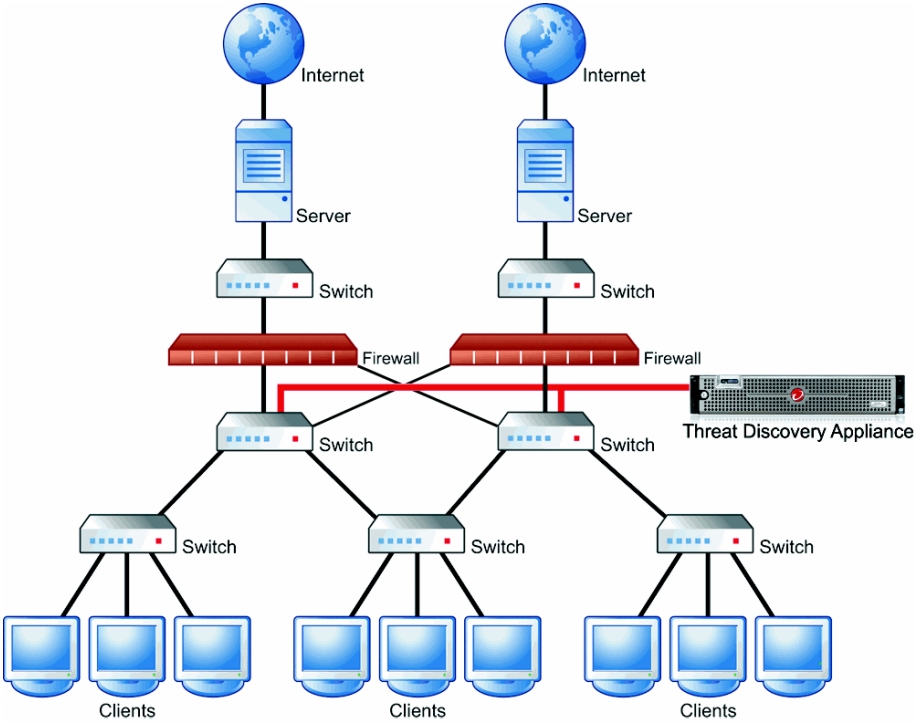


FIGURE 2-6. Redundant network monitoring

Specific VLANs

Some enterprise environments limit port scanning to specific VLANs. This can save some bandwidth and can be less resource intensive. In this scenario, Threat Discovery Appliance connection to the switches remains the same but the mirror configuration should be VLAN based.

Remote Port or VLAN Mirroring

Use remote mirroring for the following scenarios:

- Monitoring switches
- Local switch does not have enough physical ports
- Port speed on local switches do not match (GB/MB)

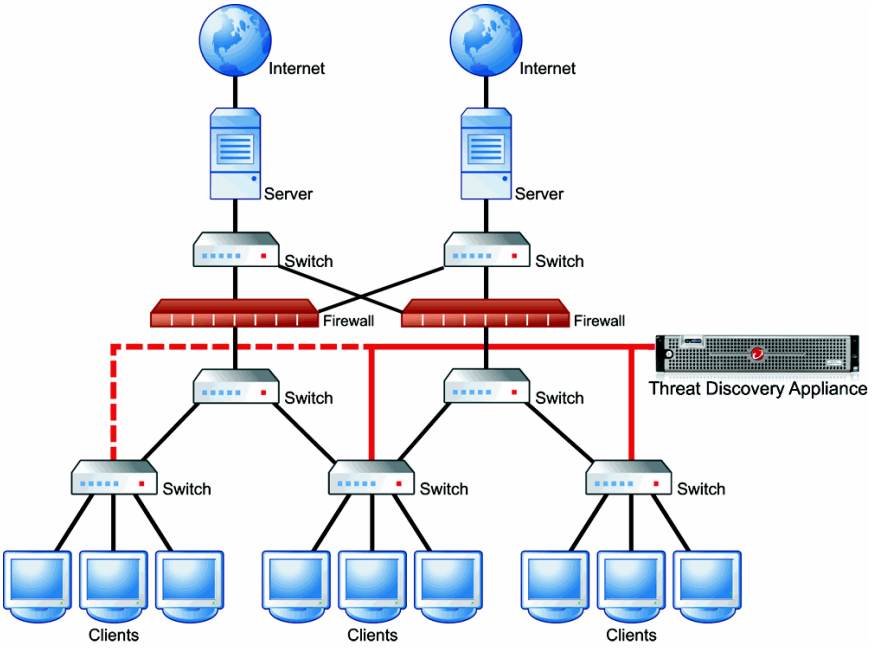


FIGURE 2-7. Remote port or VLAN mirroring

Mirroring Trunk Links

In some instances, mirror the source port from a trunk link, which means there are multiple encapsulated VLANs in the same physical link. In this scenario, ensure that the switch mirrors the correct VLAN tag to Threat Discovery Appliance for both directions.

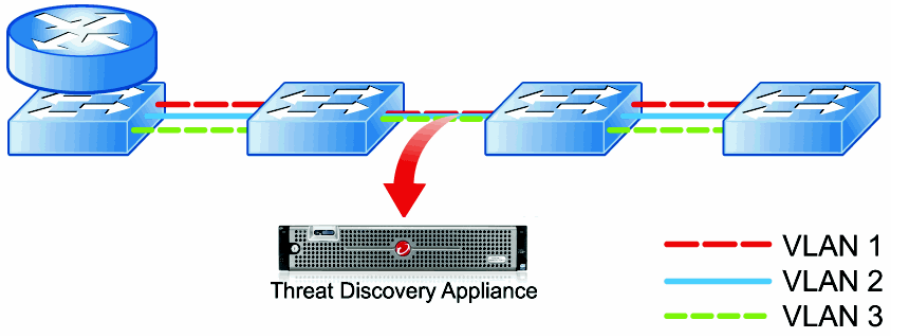


FIGURE 2-8. Mirroring trunk links

Chapter 3

Installing Threat Discovery Appliance

This chapter details the steps for installing the software appliance.

The topics discussed in this chapter are as follows:

Installation Overview

This Threat Discovery Appliance version is available as a software appliance and only supports fresh installations. Users who have previously set up an appliance or virtual appliance can upgrade to this version by performing a fresh installation of the software appliance. Back up configuration and other settings before upgrading. For details, see *Configuration Backup and Restore* on page 8-3.

The software appliance is packaged as an ISO file, and installs on a purpose-built, hardened, performance-tuned 32-bit Linux operating system that is included in the package.

Install the software appliance on a bare metal server or a VMware virtual machine that meets the requirements listed in *System Requirements* on page 3-2. The bare metal installation boots from the Threat Discovery Appliance installation CD (which contains the ISO file) to begin the process, while the VMware installation requires connecting the virtual CD/DVD drive to the installation CD or the ISO file.

WARNING! **The installation process formats the existing system to install Threat Discovery Appliance. Any existing data or partitions are removed during installation. Back up any existing data on the system before installation.**

System Requirements

Threat Discovery Appliance requires the following:

TABLE 3-1. System requirements

RESOURCES	REQUIREMENTS
Host machine	• **CPU:** Two Intel™ Core™2 Quad processors recommended • **RAM:** 2GB minimum, 4GB recommended • **Hard disk space:** 6.5GB minimum, 80GB recommended • **Network interface card (NIC):** Two NICs

TABLE 3-1. System requirements

RESOURCES	REQUIREMENTS
Preconfiguration console	Access to the Preconfiguration console requires the following: **For VGA connection:** • Monitor with a VGA port • VGA cable **For SSH connection:** • Computer with an Ethernet port • General Ethernet cable • SSH communication application such as PuTTY **For serial connection:** • Computer with a serial port • RS232 serial cable • Serial communication application such as HyperTerminal
Web-based console	Access to the web-based console requires any of the following browsers: • Microsoft Internet™ Explorer™ 6.0, 7.0, or 8.0 • Mozilla™ FireFox™ 3.0 or later

Installing Threat Discovery Appliance

This topic discusses how to install the product on a bare metal server or a VMware virtual machine.

To install Threat Discovery Appliance:

1. Perform the following steps if installing on a bare metal server:
   a. Insert the Threat Discovery Appliance installation CD into the CD/DVD drive.
   b. Power on the bare metal server and then boot from the installation CD.
2. Perform the following steps if installing on a VMware virtual machine:

WARNING! **If you install on a VMware ESX server, disable the snapshot feature for the virtual machine because the snapshot might exhaust hard disk space.**

---

   a. Create a virtual machine on the VMware ESX server. For details, see *Creating a New Virtual Machine* on page A-2.
   b. Start the virtual machine.
   c. Perform any of the following steps:
      - Insert the installation CD into the physical CD/DVD drive of the ESX server, and then connect the virtual CD/DVD drive of the virtual machine to the physical CD/DVD drive.
      - Connect the virtual CD/DVD drive of the virtual machine to the ISO file.
   d. Restart the virtual machine by clicking **VM > Send Ctrl+Alt+Del** on the VMware web console.

3. When the Welcome screen displays, press [Enter].

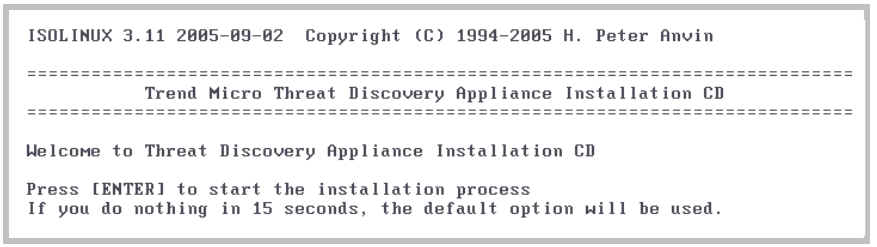


FIGURE 3-1. Welcome screen

4. When the main menu displays, perform the following steps:

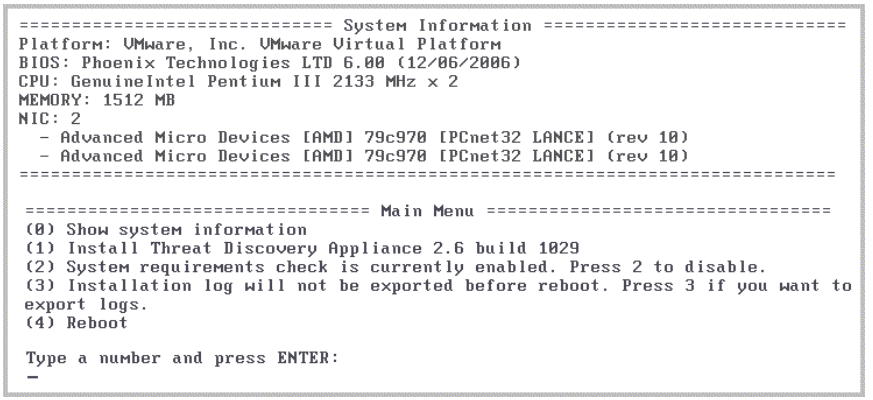


FIGURE 3-2. Main menu screen

a. By default, the installer will perform a system requirements check before installing Threat Discovery Appliance to confirm that the host machine has the necessary resources to run the product. If the purpose of installation is to test the product in a controlled environment before deploying it to your network, you can skip the system requirements check by typing **2** and pressing [Enter] .

b. To obtain installation logs that can be used for troubleshooting installation problems:

- Type **3** and press [Enter].
- Prepare a storage device, such as a removable USB flash drive, and connect it to the host machine before proceeding to the next steps.

c. Type **1** and press [Enter] to begin the installation. The installation CD (if used) is then ejected from the CD/DVD drive. Remove the CD to prevent reinstallation.

5. Threat Discovery Appliance automatically detects the active link cards (indicated by "Link is UP") that can be used for the management port. Perform the following steps:

a. Verify that the network port status indicated in this screen and the actual port's status match. If there is a status conflict, select **Re-detect** and press [Enter] to refresh the status.

b. Read the instructions if unsure which active link card is connected to your management domain.

c. Select an active link card and then press [Enter].

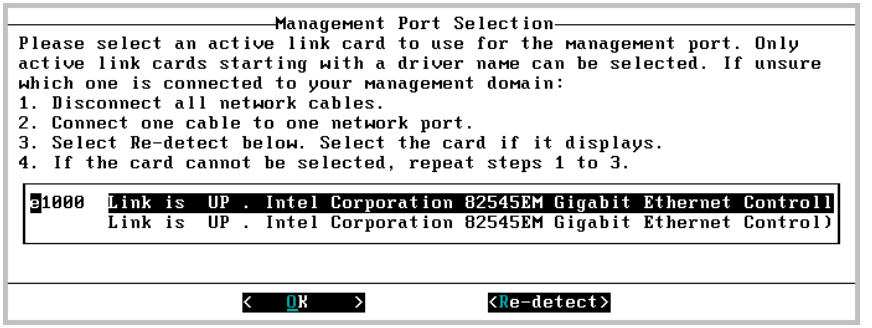


FIGURE 3-3. Management port selection screen

The installation continues.

6. When the installation is complete and you enabled the collection of installation logs in a previous step, a list of storage devices displays. Perform the following steps:

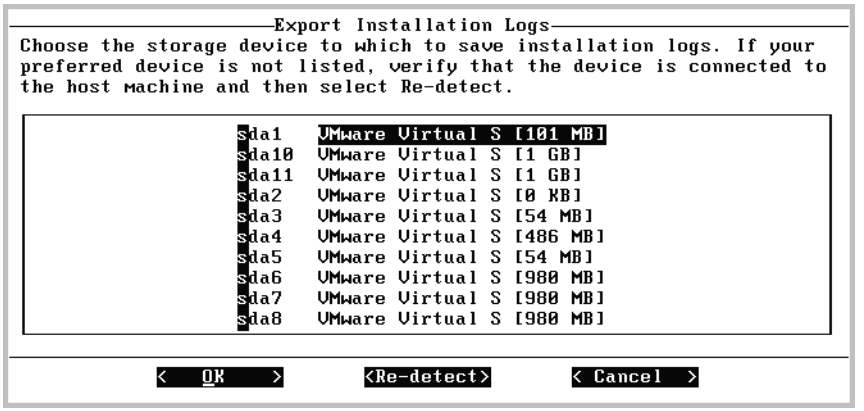


FIGURE 3-4. Export installation logs screen

   a. Select a device to which to save the logs and press [Enter]. When the installation log's file name appears, press [Enter].

Tip: Record the file name for your reference. The file name is in the following format: `install.log.YYYY-MM-DD-hh-mm-ss`

---

   b. If your preferred device is not listed, verify that the device is connected to the host machine, navigate to **Re-detect**, and press [Enter] to refresh the list.

   c. If you do not want to collect installation logs, navigate to **Cancel** and press [Enter].

   The system automatically restarts. Upon restart, the Preconfiguration Console displays.

7. Perform the necessary preconfiguration tasks for the product to be fully functional. For details, see *The Preconfiguration Console* on page 4-2.

Chapter 4

The Preconfiguration Console

This chapter explains how to use the Preconfiguration console to perform initial configuration and maintenance tasks.

The topics discussed in this chapter are:

The Preconfiguration Console

The Preconfiguration Console is a terminal communications program that allows you to configure or view any preconfiguration setting. These settings include:

- Network settings
- System logs

Use the Preconfiguration Console to do the following:

- Configure initial settings, such as the product's IP address and host name
- Restart the product
- View system logs

Note: Do not enable scroll lock on your keyboard when using HyperTerminal or you will not be able to enter data.

Preconfiguration Console Access

This topic discusses how to access the Preconfiguration Console.

To access the Preconfiguration Console:

1. There are several ways to access the Preconfiguration Console.

   From a monitor with a VGA port:

   Connect the VGA port to the VGA port of the software appliance using a VGA cable.

   From a computer with an Ethernet port:

   a. Connect the Ethernet port to the management port of the software appliance using a general Ethernet cable.

b. On the computer, open an SSH communication application such as PuTTY.

> **Note:** To connect to the software appliance from another computer in your network (not directly connected to the software appliance), ensure that you access the computer connected to the management port.

c. Use the following values if you are accessing the console for the first time:

- IP address (for SSH connection only): by default, it is 192.168.252.1
- User name: tda
- Password: press [Enter]
- Port number: 22

From a computer with a serial port:

a. Connect the serial port to the serial port of the software appliance using an RS232 serial cable.

b. On the computer, open a serial communication application such as HyperTerminal.

c. Use the following values if you are accessing the console for the first time:

- Bits per second: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

2. When the Preconfiguration Console screen opens, type the default password **admin** and press [Enter] twice.

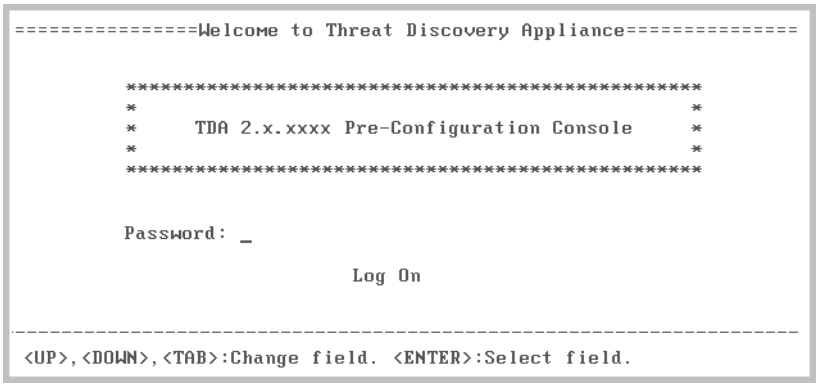


FIGURE 4-1. The Logon screen

Preconfiguration Menu

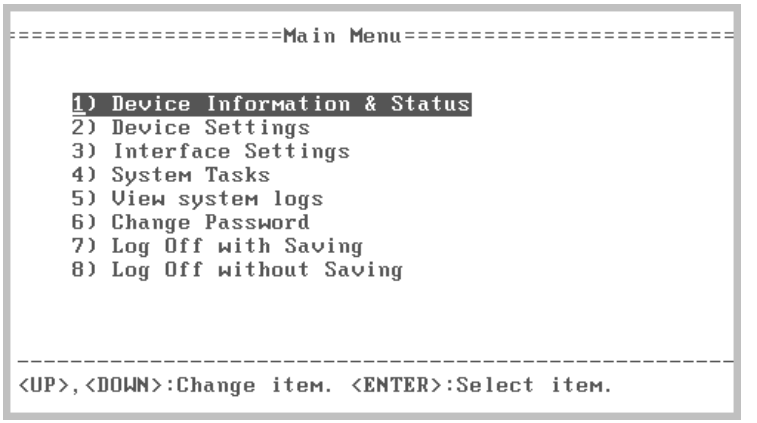


FIGURE 4-2. The Preconfiguration Console's main menu

The Preconfiguration Console menu displays the following:

TABLE 4-1. Main menu item descriptions

MENU ITEMS	DESCRIPTION
Device Information and Status	View product information and monitor memory usage.
Device Settings	Modify the product's host name, IP address, subnet mask, and the network default gateway address and DNS servers. You can register Threat Discovery Appliance to Trend Micro Control Manager for centralized management.
Interface Settings	View the network speed and duplex mode for the management port, which Threat Discovery Appliance automatically detects.
System Tasks	Roll back to the previous update, perform a diagnostic test, or restart the product. You can also import or export the configuration file and import the HTTPS certificate.
View System Logs	View logs detailing security risks and incidents.
Change Password	Change the root password.
Log Off with Saving	Log off from the Preconfiguration Console after saving the changes.
Log Off without Saving	Log off from the Preconfiguration Console without saving the changes.

To access a menu item, type the number for the menu item and then press [Enter].

Preconfiguration Menu: Device Information and Status

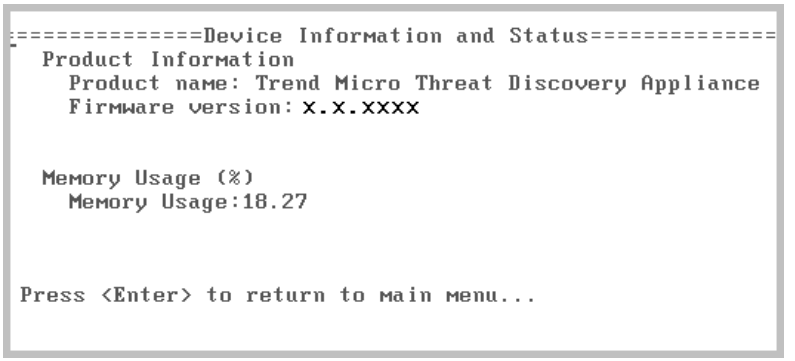


FIGURE 4-3. The Device Information and Status screen

View the product name, program version, and memory usage from this screen. You can also view memory usage information from the web-based console's Summary screen. For details, see *Product Summary* on page 7-5.

To view product information:

1. Log on to the Preconfiguration Console. The Main Menu appears.
2. Type **1** to select **Device Information & Status** and press [Enter]. The Device Information and Status screen appears.
3. Press [Enter] to return to the main menu.

Preconfiguration Menu: Device Settings

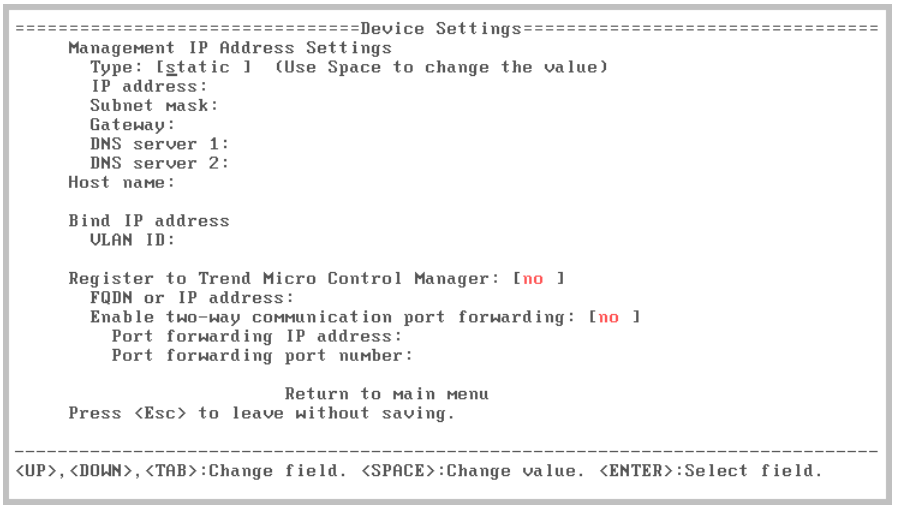


FIGURE 4-4. The Device Settings screen

Use the Device Settings screen to configure the management IP address settings and register Threat Discovery Appliance to Trend Micro Control Manager.

These tasks can also be performed on the web-based console.

To modify settings using the Preconfiguration Console:

1. Log on to the Preconfiguration Console. The Main Menu appears.
2. Type **2** to select **Device Settings** and press [Enter]. The Device Settings screen appears.
3. Configure IP address settings.

   To use dynamic IP address:

   a. In the **Type** field, use the space bar to change the IP address option from **static** to **dynamic**.

To use static IP address:

a. In the **Type** field, use the space bar to change the IP address option from **dynamic** to **static**.

b. Type a new **IP address**, **Subnet mask**, **Default gateway** IP address, and **Primary** and **Secondary DNS server** IP addresses.

4. Type a new host name.
5. (Optional) Type a VLAN ID.
6. (Optional) Register to Trend Micro Control Manager.

Note: You can also use the web-based console to register to Control Manager.

---

a. In the **Register to Trend Micro Control Manager** field, use the space bar to change the option to **[yes]**.

b. Type the Control Manager IP address.

c. In the **Enable two-way communication port forwarding** field, use the space bar to set the option to **[no]** or **[yes]**.

d. To enable two-way communication between Threat Discovery Appliance and Control Manager, type the IP address and pot number of your router or NAT device in the **Port forwarding IP address** and **Port forwarding port number** fields.

Note: Configuring the NAT device is optional and depends on the network environment. For more information on NAT, refer to the *Trend Micro Control Manager Administrator's Guide*.

---

7. Navigate to **Return to main menu** and press [Enter] to return to the main menu.
8. Type **7** and press [Enter] to save the settings.

Preconfiguration Menu: Interface Settings

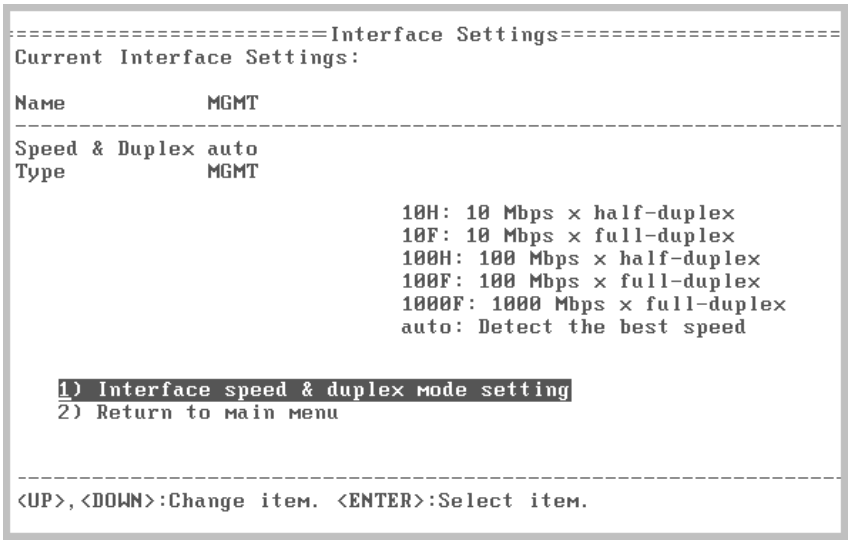


FIGURE 4-5. The Interface Settings screen

By default, Threat Discovery Appliance automatically detects the network speed and duplex mode for the management port (MGMT), so it is unlikely that you need to change this setting. However, if any issues with the connection arise, you can manually configure these settings.

Tip: To maximize throughput, Trend Micro recommends full-duplex mode.

Half-duplex is acceptable. However, network throughput is limited because half-duplex communication requires any computer transmitting data to wait and retransmit if a collision occurs.

Note: Data ports used by the product can be managed from the web-based console by navigating to **Administration > Network Interface Settings**. For details, see *Network Interface Settings* on page 5-5.

To modify interface settings:

1. Log on to the Preconfiguration Console. The Main Menu appears.
2. Type **3** to select **Interface Settings** and press [Enter]. The Interface Settings screen appears.
3. To change the interface settings:
   a. Type **1** and press [Enter].
   b. In the **Speed and Duplex** field, use the space bar to change the network speed and duplex mode.
   c. Navigate to **Return to main menu** and press [Enter].
4. Type **2** and press [Enter] to return to the main menu.
5. Type **7** and press [Enter] to save the settings.

Preconfiguration Menu: System Tasks

Use the System Tasks screen if you encounter an error message that requires you to roll back the Threat Discovery Appliance update, or if you need to import or export the configuration file, import the HTTPS certificate or restart the product.

Tip: Importing and exporting the configuration file can also be performed from the web-based console.

Perform the following tasks:

- *Rolling back to the Previous Update* on page 4-10
- *Importing the Configuration File* on page 4-12
- *Exporting the Configuration File* on page 4-14
- *Importing the HTTPS Certificate* on page 4-16
- *Performing a Diagnostic Test* on page 4-17
- *Restarting Threat Discovery Appliance* on page 4-17

Rolling back to the Previous Update

If an update causes operational problems or is not compatible with Threat Discovery Appliance, roll back to the previous update.

To roll back to the previous update:

1. Log on to the Preconfiguration Console. The Main Menu appears.
2. Type **4** and press [Enter]. The System Tasks screen appears.

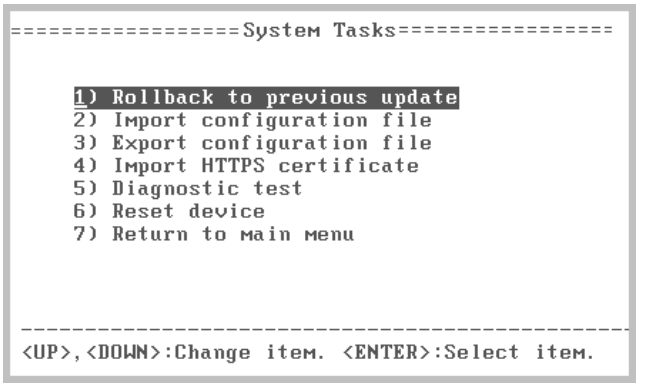


FIGURE 4-6. The System Tasks screen

3. Type **1** and press [Enter]. The Rollback to previous update screen appears.

Note: Rolling back to previous update may require restarting the product.

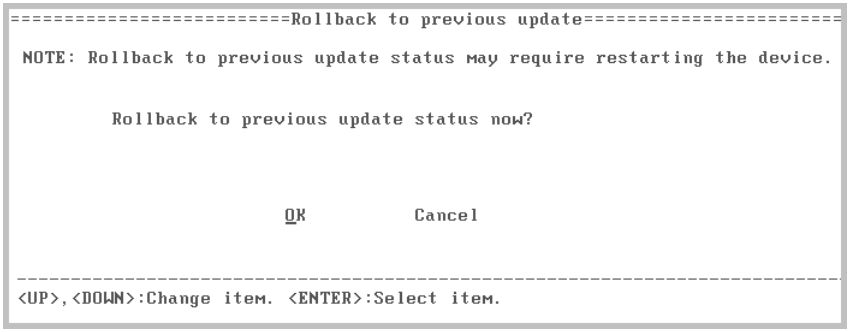


FIGURE 4-7. The Rollback to previous update screen

4. Select **OK** and press [Enter]. The product rolls back to the previous updates.

Importing the Configuration File

If the software appliance encounters errors with the current settings, you can restore the configuration and database from a backup file.

WARNING! **Export the current configuration settings before importing the backup configuration file. For details, see** *Exporting the Configuration File* **on page 4-14).**

To import the backup configuration file:

1. Log on to the Preconfiguration Console. The Main Menu appears.
2. Type **4** and press [Enter]. The System Tasks screen appears.
3. Type **2** and press [Enter]. The Import configuration file screen appears.
4. From the HyperTerminal menu, click **Transfer > Send File**.

Note: The **Send File** option means sending the file to the software appliance before you can import it.

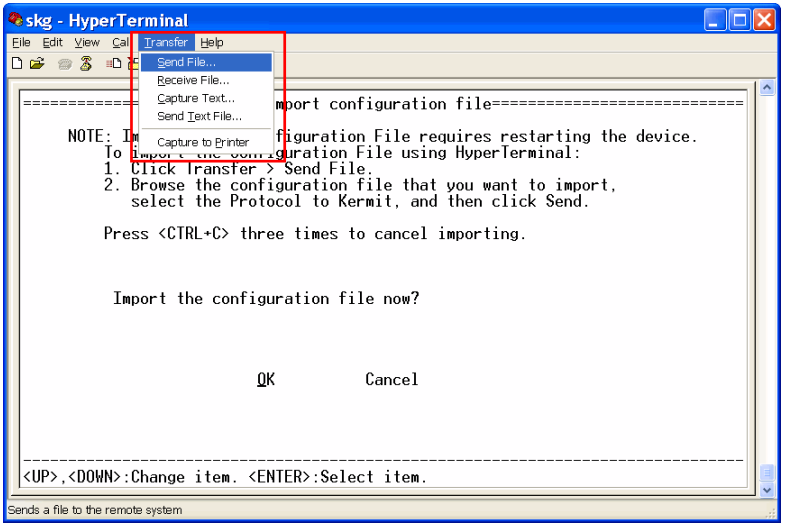


FIGURE 4-8. Preconfiguration Console send file screen

5. Browse to the configuration file to import.

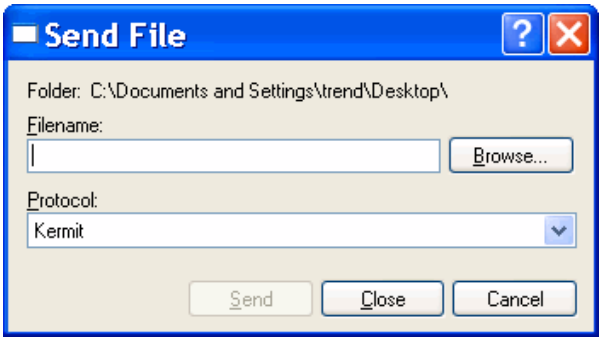


FIGURE 4-9. Send file screen

6. Change the protocol to **Kermit** and then click **Send**.

Tip: Trend Micro recommends exporting the current configuration settings before importing the backup configuration file.

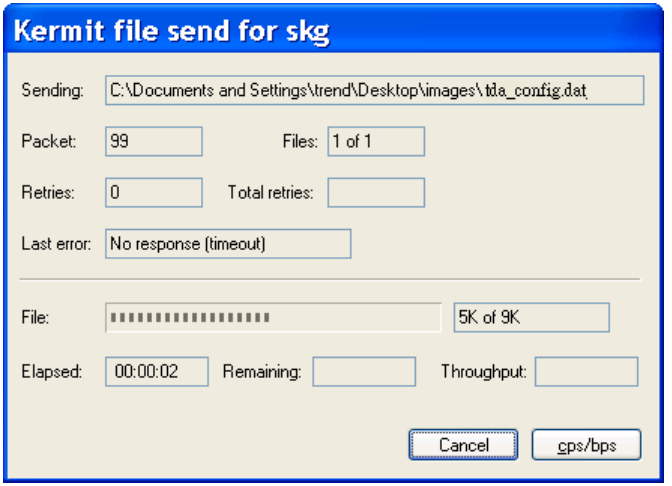


FIGURE 4-10. Kermit file send screen

7. The software appliance imports the configuration file and uses the settings from the file.

Exporting the Configuration File

Regularly back up the configuration files to ensure that you use the latest configuration settings.

To export the configuration file:

1. Log on to the Preconfiguration Console. The Main Menu appears.
2. Type **4** and press [Enter]. The System Tasks screen appears.
3. Type **3** and press [Enter]. The Export configuration file screen appears.
4. From the HyperTerminal menu, click **Transfer > Receive File**.

Note: The **Receive File** option means receiving the file from the software appliance before exporting.

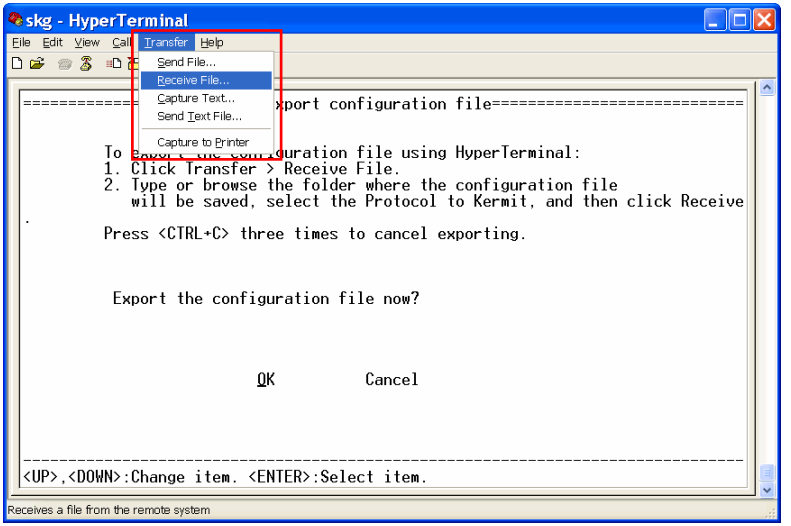


FIGURE 4-11. Preconfiguration Console receive file screen

5. Browse to the configuration file to export.

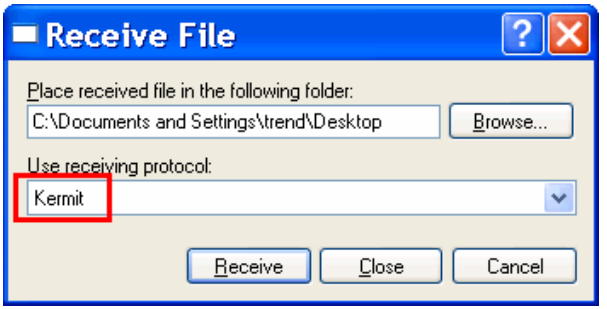


FIGURE 4-12. Receive file screen

6. Change the protocol to **Kermit**, and then click **Receive**.

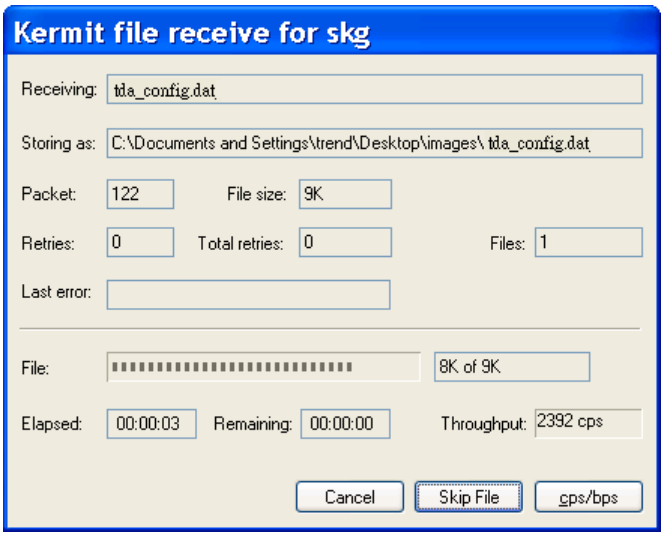


FIGURE 4-13. Kermit file receive screen

7. The software appliance exports the configuration settings to a `.dat` file.
8. Rename the exported configuration files to keep track of the latest configuration files.

Importing the HTTPS Certificate

This task enables administrators to import security certificates from a well-known Certificate Authority (CA). This eliminates browser security issues that may occur when using the default certificate delivered with Threat Discovery Appliance.

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 import the HTTPS certificate:

1. Log on to the Preconfiguration Console. The Main Menu appears.
2. Type **4** and press [Enter]. The System Tasks screen appears.
3. Type **4** and press [Enter]. The Import HTTPS certificate screen appears.

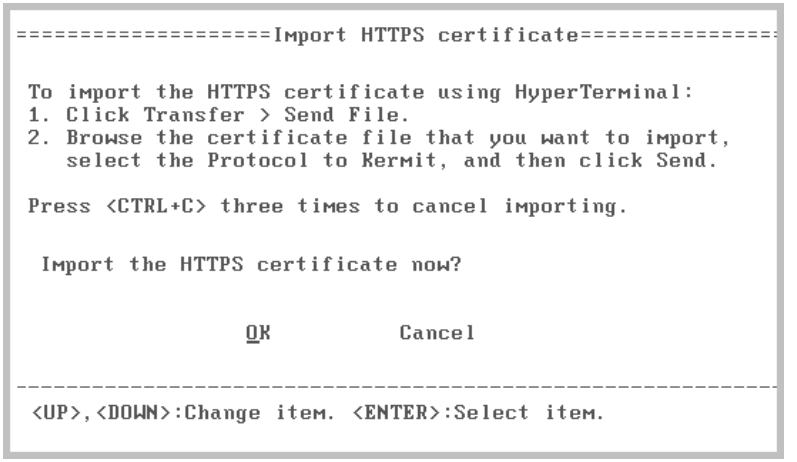


FIGURE 4-14. The Import HTTPS Certificate screen

4. From the HyperTerminal menu, click **Transfer > Send File**.
5. Browse to the HTTPS certificate file you want to import.
6. Change the Protocol to Kermit, then click **Send**.

Performing a Diagnostic Test

Use this feature to perform diagnostic tests of the system and application. This helps determine if there are any software issues.

To perform the diagnostic test:

1. Log on to the Preconfiguration Console. The Main Menu appears.
2. Type **4** and press [Enter]. The System Tasks screen appears.
3. Type **5** and press [Enter]. The Diagnostic Test screen appears.
4. From the HyperTerminal menu, click **Transfer > Capture Text**.
5. Browse to the folder and specify the file name for the log.
6. Click **Start**.
7. Under **Run diagnostic test now?**, navigate to **OK** and press [Enter].
8. After Threat Discovery Appliance restarts, open the captured log to view the log result.

Restarting Threat Discovery Appliance

To restart the software appliance, access the Preconfiguration Console using a serial communication application such as HyperTerminal or an SSH utility such as PuTTY. Using PuTTY to access the Preconfiguration Console means you can restart the software appliance remotely.

When Threat Discovery Appliance starts, it checks the integrity of its configuration files. The web-based console password may reset if the configuration file containing password information is corrupted. If you are unable to log on to the console using your preferred password, log on using the default password **admin**.

To restart Threat Discovery Appliance:

1. Log on to the Preconfiguration Console. The Main Menu appears.
2. Type **4** and press [Enter]. The System Tasks screen appears.
3. Type **6** and press [Enter]. The Reset Device screen appears.
4. Under **Reset Trend Micro Threat Discovery Appliance and keep current configuration**, navigate to **OK** and press [Enter].

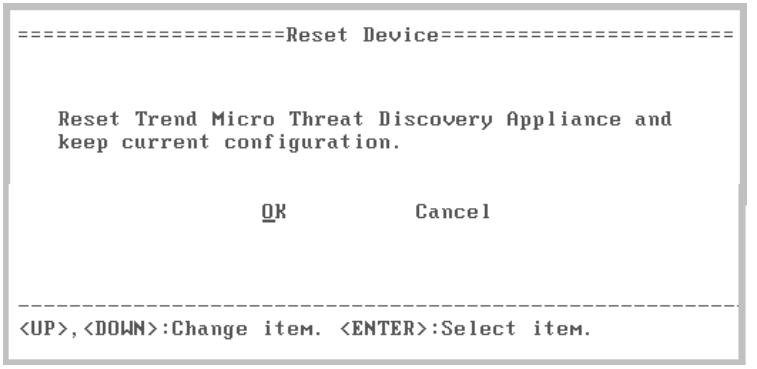


FIGURE 4-15. The Reset Device screen

Threat Discovery Appliance restarts.

Preconfiguration Menu: View System Logs

FIGURE 4-16. An example of a System log

The log format in the Preconfiguration Console displays the logs. For more organized and configurable logs, use the Detection Log Query on the web-based console. For details, see *Detection Logs* on page 7-24.

To view system logs in the Preconfiguration Console:

1. Log on to the Preconfiguration Console. The Main Menu appears.
2. Type **5** and press [Enter]. The System log screen appears.

> **Note:** You will initially see a blank screen. Wait for a couple of seconds. The logs appear as soon as Threat Discovery Appliance detects activity in the network.

Preconfiguration Menu: Change Password

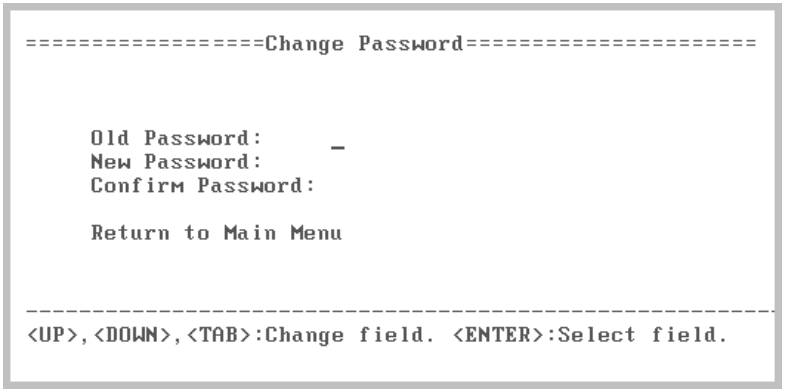


FIGURE 4-17. The Change Password screen

Change the Threat Discovery Appliance password using the Preconfiguration Console.

To change the root password in the Preconfiguration Console:

1. Log on to the Preconfiguration Console. The Main Menu appears.
2. Type **6** and press [Enter]. The Change Password screen appears.
3. Type the old and new passwords.
4. Confirm the new password.
5. Navigate to **Return to main menu** and press [Enter] to return to the main menu and save the settings.

Preconfiguration Menu: Log Off

You have 2 options when logging off from the Preconfiguration Console:

Log off with Saving

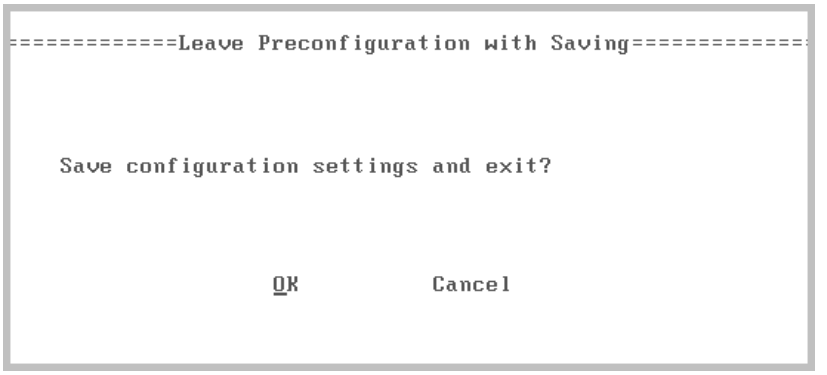


FIGURE 4-18. The Leave Preconfiguration with Saving screen

Log off without Saving

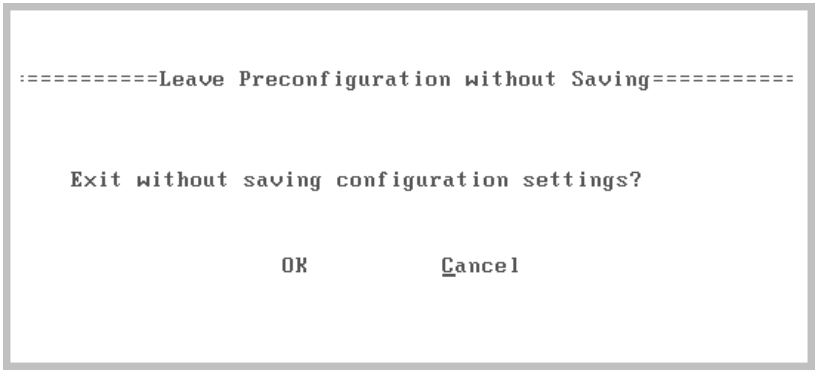


FIGURE 4-19. The Leave Preconfiguration without Saving screen

To log off and save:

Note: Some tasks, such as changing the password and resetting the product, are automatically saved and therefore do not require going through this process.

1. After making changes to the configuration settings, return to the main menu.
2. Type **7** and press [Enter]. The Leave Preconfiguration with Saving screen appears.
3. Under **Save configuration settings and exit?**, navigate to **OK** and press [Enter].

To log off without saving:

1. After making any changes to the configuration settings, return to the main menu.
2. Type **8** and press [Enter]. The Leave Preconfiguration without Saving screen appears.
3. Under **Exit without saving configuration settings?**, navigate to **OK** and press [Enter].

Chapter 5

Getting Started

This chapter introduces the settings you need to configure immediately after setting up Threat Discovery Appliance.

The topics discussed in this chapter are:

Network Settings

The following format rules apply to Threat Discovery Appliance network settings.

Host Name Format

Use the Fully Qualified Domain Name (FQDN) for the host name; for example:

`hostname.domain_1.com`

The host name can contain alphanumeric characters and dashes ("A-Z", "0-9", "-").

IP Address Format

IP addresses must be in the format: `XXX.XXX.XXX.XXX`, where x is a decimal value between 0 and 255. The IP address cannot be in any of the following formats:

- `AAA.XXX.XXX.XXX`, where A is in the range 223 to 240 [Multicast Address]
- `0.0.0.0` [Local Host name]
- `255.255.255.255` [Broadcast Address]
- `127.0.0.1` [Loopback Address]

Subnet Mask Format

Subnet masks are best explained by looking at the IP address and subnet mask in its binary format. The binary format of the subnet mask starts with a sequence of continuous 1s and ends with a sequence of continuous 0s.

For example:

- For `255.255.255.0`, the binary format is `11111111.11111111.11111111.00000000.`
- For `255.255.252.0`, the binary format is `11111111.11111111.11111100.00000000.`

Default Gateway Address Format

The gateway must be in the same subnet as the IP address. The combination of the IP address and the subnet mask should not be the broadcast or network address.

VLAN ID

The VLAN ID is a valid VLAN identifier ranging from 1-4094.

Product Console

Threat Discovery Appliance provides a built-in web console through which you can configure all product settings. This section explains how to access the product console.

To open the product console:

1. From a computer in your network, open a browser window. The following browsers and versions are supported:
   - Microsoft™ Internet Explorer™ 6.0, 7.0, or 8.0
   - Mozilla™ FireFox™ 3.0 or later

   Note: To ensure that tool tips and reports appear, set the Internet Security level to Medium and enable ActiveX Binary and Script Behaviors.

2. Using the managed port IP address you set for the product during initial configuration, type the following URL:

   https://192.168.252.1/index.html

   Note: The URL is case sensitive. Type the URL exactly as it appears.

3. Type the default password: **admin**

   Note: Change the password immediately after logging on for the first time (see *Product Console Password* on page 5-4).

4. Click **Log On**.

   Note: If you change the product IP address, update your browser bookmark to access the product console at the new IP address.

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 should be a mixture of alphanumeric characters such as 0-9, a-z, A-Z, !$%^ and must be 4 to 32 characters long.

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 > PASSWORD

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

Network Interface Settings

The Network Interface Settings screen allows you to manage the product's IP address and network interface ports.

Threat Discovery Appliance requires its own IP address to ensure that the management port can access the product console. If there is a DHCP server on your network and you want it to dynamically assign an IP address to Threat Discovery Appliance, select Dynamic IP address (DHCP). Otherwise, select static IP address.

Threat Discovery Appliance uses a management port and several data ports. You can view the status of these ports, change the network speed/duplex mode for each of the data ports, and capture packets for debugging and troubleshooting purposes.

Note: The network speed/duplex mode for the management port can only be configured from the Preconfiguration Console. For details, see *Preconfiguration Menu: Interface Settings* on page 4-9.

To configure a dynamic IP address:

PATH: ADMINISTRATION > NETWORK INTERFACE SETTINGS > APPLIANCE IP ADDRESS SETTINGS

1. In **Appliance Host Name**, specify the host name.
2. Select **Dynamic IP Address (DHCP)**.
3. Click **Save**.

To configure a static IP address:

PATH: ADMINISTRATION > NETWORK INTERFACE SETTINGS > APPLIANCE IP ADDRESS SETTINGS

1. In **Appliance Host Name**, specify the host name.
2. Select **Static IP address**.
3. Type the following:
   - **IP address:** The numeric address specifically for Threat Discovery Appliance
   - **Subnet Mask:** Indicates the subnet mask for the network to which the Threat Discovery Appliance IP address belongs
   - (Optional) **Gateway:** The IP address of the network gateway

- (Optional) **DNS Server 1:** The IP address of the primary server that resolves host names to an IP address
- (Optional) **DNS Server 2:** The IP address of the secondary server that resolves host names to an IP address

4. Click **Save**.

To manage network interface ports:

PATH: ADMINISTRATION > NETWORK INTERFACE SETTINGS > NETWORK INTERFACE PORTS

1. View the status for each port.
2. To change the port's network speed and duplex mode, select from the options under **Connection Type**.
3. Select **Check VLAN tags** if VLAN tags are used to differentiate TCP connections.
4. To capture packets on each port, click **Start** under **Packet Capture**. The date/time of the packet capture session displays next to the button. The total amount of packets captured dynamically displays on the lower section of the screen.

   Note: It is not possible to run multiple capture sessions. Wait for a session to finish before starting a new one.

5. Click **Stop** if the packet capture session is done.

   Note: The maximum size of the file containing packet data is 30MB.

6. To view data for the particular packet capture session, click **View**.
7. To export the data to a log file, click **Export** and then specify the target location of the log file **tcpdump.tgz**.

   Tip: Send the log file to Trend Micro if you need troubleshooting assistance.

8. To remove files containing packet data, click **Reset**.

System Time

Synchronize the system time with the Network Time Protocol (NTP) server, or manually configure the time.

To set the system time:

PATH: ADMINISTRATION > SYSTEM TIME

1. Under System Time Settings, select either of the following:
   - Synchronize appliance time with an NTP server; or
     i. In **NTP Server**, type the NTP server address.
     ii. Click **Synchronize Now**.
   - Manually set the system time
     i. Type the month, day, and year using the mm/dd/yy format.
     ii. Select the hour, minute, and second.
2. Under **Time zone**, select the appropriate time zone from the list of standard time zones.
3. Click **Save**.

Proxy Settings

Threat Discovery Appliance uses the proxy settings configured in the web-based console when it performs the following tasks:

- Download updates from the Trend Micro ActiveUpdate server or another update source
- Update the product license
- Connect to other Trend Micro products such as TMSP, Smart Protection Server, and Control Manager

To configure proxy settings:

PATH: ADMINISTRATION > PROXY SETTINGS

1. Select **Use a proxy server for pattern, engine, and license updates**.
2. Select **HTTP**, **SOCKS4**, or **SOCKS5** for the **Proxy protocol**.
3. Type the server name or IP address and the port number. For example, type `192.1.1.1` as the server IP address and `1234` as the port number.
4. If your proxy server requires authentication, type the **User name** and **Password** under **Proxy server authentication**.
5. Click **Test Connection** to verify connection settings.
6. Click **Save** if connection was successful.

Licenses and Activation Codes

The Product License screen displays license information and accepts valid Activation Codes for Threat Discovery Appliance and Security Compliance.

Note: Security Compliance is an optional, separately licensed feature and can only be activated if Threat Discovery Appliance has been activated. For more information, see *Security Compliance* on page 6-18.

Activation Codes

Use a valid Activation Code to enable your Trend Micro product. A product will not be operable until activation is complete. An Activation Code has 37 characters (including the hyphens) and appears as follows:

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

If you received a Registration Key instead of an Activation Code, use it to register Threat Discovery Appliance or Security Compliance at:

https://olr.trendmicro.com/registration/

A Registration Key has 22 characters (including the hyphens) and appears as follows:
`xx-xxxx-xxxx-xxxx-xxxx`

After registration, you will receive an Activation Code through email.

Fully Licensed and Evaluation Versions

Depending on the Activation Code that you received from Trend Micro, you might have a fully licensed or an evaluation version of Threat Discovery Appliance or Security Compliance.

- **Fully licensed version:** Includes all the product features and technical support. A 30-day grace period takes effect after the license expires. Renew the license before it expires by purchasing a maintenance renewal.
- **Evaluation version:** Includes all the product features. Upgrade an evaluation version to the fully licensed version at any time.

License status displays on top of the Product License screen. If you are renewing a license and need renewal instructions, click **View renewal instructions** beside the status information.

The status includes reminders when a license is about to expire or has expired.

- For an evaluation version, a reminder displays when the license expires. The consequences of not upgrading to the fully licensed version are listed in *Table 5-1*.
- For a fully licensed version, a reminder displays:
  - 60 days before expiration ends
  - 30 days before grace period ends
  - When the license expires and grace period elapses. The consequences of not renewing the license are listed in *Table 5-1*.

TABLE 5-1. Consequences of an expired license

LICENCE TYPE AND STATUS		CONSEQUENCES
THREAT DISCOVERY APPLIANCE	SECURITY COMPLIANCE	
Evaluation (Expired)	Evaluation or Fully Licensed (Valid)	• Threat Discovery Appliance disables component updates, scanning, and log transmission to TMSP. • Security Compliance stops working.
	Evaluation or Fully Licensed (Expired)	
Fully Licensed (Expired)	Evaluation or Fully Licensed (Valid)	• You will not be able to obtain technical support and perform component updates. • Threat Discovery Appliance will still monitor the network using out-of-date components. These components may not be able to completely protect you from the latest security risks. • Security Compliance continues to work.

TABLE 5-1. Consequences of an expired license (Continued)

LICENCE TYPE AND STATUS		CONSEQUENCES
THREAT DISCOVERY APPLIANCE	SECURITY COMPLIANCE	
Fully Licensed (Expired)	Evaluation or Fully Licensed (Expired)	• You will not be able to obtain technical support and perform component updates. • Threat Discovery Appliance will still monitor the network using out-of-date components. These components may not be able to completely protect you from the latest security risks. • Security Compliance stops working.
Evaluation or Fully Licensed (Valid)	Evaluation or Fully Licensed (Expired)	• Security Compliance stops working.

To activate or renew a license:

PATH: ADMINISTRATION > PRODUCT LICENSE

1. Click **New Activation Code**. The New Activation Code screen displays.
2. Type the new Activation Code and click **Save**. The Trend Micro License Agreement displays.
3. Read the license agreement and click **Agree**.

> **Note:** If you activated Threat Discovery Appliance, the Setup Guide displays. Follow the steps in the Setup Guide.

4. From the Product License Details screen, click **Update Information** to refresh the screen with the new license details. This screen also provides a link to your detailed license available on the Trend Micro website.

Component Updates

Download and deploy product components used to scan for and detect network threats. Because Trend Micro regularly creates new component versions, perform regular updates to address the latest Internet threats.

Components

To help protect your network, Threat Discovery Appliance uses the components listed in *Table 5-2*.

TABLE 5-2. Threat Discovery Appliance Components

COMPONENT	DESCRIPTION
Virus Scan Engine	Enables the product to scan for viruses and Trojans.
Virus Pattern	Used for identifying virus signatures—unique patterns of bits and bytes that signal the presence of a virus.
Spyware Active-monitoring Pattern	Used for identifying unique patterns of bits and bytes that signal the presence of certain types of potentially undesirable files and programs, such as adware and spyware, or other grayware.
IntelliTrap Pattern	Used for identifying real-time compressed executable file types that commonly hide viruses and other potential threats.
IntelliTrap Exception Pattern	Provides a list of real-time compressed executable file types that are commonly safe from viruses and other potential threats.
Network Content Inspection Engine	The engine used to perform network scanning.
Network Content Inspection Pattern	The pattern used by the Network Content Inspection Engine to perform network scanning.
Network Content Correlation Pattern	The pattern used by the Network Content Correlation Engine that implements rules defined by Trend Micro.

TABLE 5-2. Threat Discovery Appliance Components (Continued)

COMPONENT	DESCRIPTION
Threat Discovery Appliance Firmware	The program file used on by Threat Discovery Appliance. **Tip:** Trend Micro recommends using the Firmware Update screen when updating the firmware.

Update Methods

There are several ways to update components:

TABLE 5-3. Update methods

METHOD	DESCRIPTION
Manual update	When you click **Updates > Manual** on the main menu, Threat Discovery Appliance checks if any components are out of date and gives you the option to update the components (see *Manual Updates* on page 5-15). **Note:** Threat Discovery Appliance updates all components. You cannot update components individually.
Scheduled update	When you configure an update schedule, Threat Discovery Appliance automatically checks the update source at the frequency you specify (see *Scheduled Updates* on page 5-16). Scheduled update relieves you of the task of manually keeping components up-to-date.
Firmware update	Threat Discovery Appliance provides a separate screen for updating the firmware by clicking **Administration > Firmware Update** on the main menu. For details, see *Firmware Update* on page 8-5.

Update Tasks

To update components successfully, follow the procedures outlined in the following topics:

1. *Proxy Settings* on page 5-8
2. *Update Source* on page 5-14
3. *Manual Updates* on page 5-15
4. *Scheduled Updates* on page 5-16

Update Source

Threat Discovery Appliance downloads components from the Trend Micro ActiveUpdate server, the default update source. You can also configure Threat Discovery Appliance to download components from another update source, such as a custom update source specifically set up in your organization.

Note: You can configure Threat Discovery Appliance to download directly from Control Manager. Refer to the *Trend Micro Control Manager Administrator's Guide* for more details on how a Control Manager server can act as an update source.

To configure the update source:

PATH: UPDATES > SOURCE

1. Under **Download Updates From**, select one of the following update sources:
   - **Trend Micro ActiveUpdate server:** The Trend Micro ActiveUpdate server is the default source for the latest components.
   - **Other update source:** Select this option to specify an update source different from the default source. The update source must begin with "http://" or "https://". For example, http://activeupdate.mycompany.com or https://activeupdate.mycompany.com.

     Note: Update sources cannot be specified in UNC path format.

2. (Optional) Enable **Retry Unsuccessful Updates** and then specify **Number of retry attempts** and **Retry interval**.
3. Click **Save**.

Manual Updates

Threat Discovery Appliance allows you to perform updates on demand. This is a useful feature during outbreaks, when updates do not arrive according to a fixed schedule.

The following details appear in the Manual Download screen:

TABLE 5-4. Details in the Manual Download screen

DETAILS	DESCRIPTION
Component	The component name
Current Version	The version number of each component currently used by the product
Latest Version	The latest version available on the server
Last Updated	The date and time of the last update

To perform manual updates:

PATH: UPDATES > MANUAL

1. Click **Update** to start updating components. Threat Discovery Appliance automatically checks which components need updating.
2. A **Restart** button appears at the lower section of the screen if the Network Content Inspection Engine or firmware was updated. Click **Restart** immediately.

Note: When Threat Discovery Appliance starts, it checks the integrity of its configuration files. The product console password may reset if the configuration file containing password information is corrupted. If you are unable to log on to the console using your preferred password, log on using the default password **admin**.

Scheduled Updates

Configuring an update schedule is an easy and effective way of ensuring that you always get the latest components. This minimizes your risk from security threats.

Tip: Schedule updates during off-peak hours.

If the Network Content Inspection Engine and firmware were updated during a scheduled update, you will receive an email notifying you to restart Threat Discovery Appliance. Restart the product immediately. When Threat Discovery Appliance starts, it checks the integrity of its configuration files. The product console password may reset if the configuration file containing password information is corrupted. If you are unable to log on to the console using your preferred password, log on using the default password **admin**.

To configure scheduled updates:

PATH: UPDATES > SCHEDULED

1. Select **Enable Scheduled Component Updates**.
2. Select the update schedule based on **Minutes**, **Hours**, **Days**, or **Week, on** and specify the time or day.

   Tip: Trend Micro recommends setting the update schedule to every two hours.

3. Click **Save**.

Chapter 6

Configuring Product Settings

This chapter explains how to configure Threat Discovery Appliance settings.

The topics discussed in this chapter are:

Network Configuration

Network configuration defines and establishes the profile of the network Threat Discovery Appliance monitors. Identify monitored networks, services provided, and network domains to enable the Network Content Correlation Engine to establish its knowledge of the network.

See the following topics for details:

- *Monitored Networks* on page 6-2
- *Registered Domains* on page 6-4
- *Registered Services* on page 6-5

You can replicate network configuration settings from one Threat Discovery Appliance to another by exporting the settings to a file and then importing the file to other Threat Discovery Appliances. For details, see *Network Configuration Replication* on page 6-6.

Monitored Networks

Establish groups of monitored networks using IP addresses to allow Threat Discovery Appliance to determine whether attacks originate from within or outside the network.

To add monitored networks:

PATH: NETWORK CONFIGURATION > MONITORED NETWORK

1. Click **Add**. The Add Monitored Network Group screen appears.
2. Specify a group name.

Note: Provide specific groups with descriptive names for easy identification of the network to which the IP address belongs. For example, use Finance network, IT network, or Administration.

---

3. Specify an IP address range in the text box. You can add a maximum of 1,000 IP address ranges.
   - Threat Discovery Appliance comes with a monitored network called **Default**, which contains the following IP address blocks reserved by the Internet Assigned Numbers Authority (IANA) for private networks:
     - 10.0.0.0 - 10.255.255.255
     - 172.16.0.0 - 172.31.255.255
     - 192.168.0.0 - 192.168.255.255

     If you did not remove **Default**, you do not need to specify these IP address blocks when adding a new monitored network.
   - Use a dash to specify an IP address range, such as 192.168.1.0-192.168.1.255.
   - Use a slash to specify the subnet mask for IP addresses, such as 192.168.1.0/255.255.255.0 or 192.168.1.0/24.
4. Select the **Network zone** of network group.

Note: Selecting **Trusted** means this is a secure network and selecting **Untrusted** means there is a degree of doubt on the security of the network.

---

5. Click **Add**.
6. Click **Save**.

To remove monitored networks:

PATH: NETWORK CONFIGURATION > MONITORED NETWORK

1. Select the Group Name(s) that you want to remove.
2. Click **Delete**.

Registered Domains

Add domains used by companies for internal purposes or those considered trustworthy to establish the network profile. Identifying trusted domains ensures detection of unauthorized domains.

You can add a maximum of 1,000 domains, but add only trusted domains to ensure accuracy of your network profile.

Threat Discovery Appliance supports suffix matching for registered domains. This means adding domain.com also adds one.domain.com, two.domain.com, and so on.

To add registered domains:

PATH: NETWORK CONFIGURATION > REGISTERED DOMAINS

1. Specify a domain name.
2. (Optional) Click **Analyze** to display a list of domains that you can add to the list.
3. Click **Add**.

To remove registered domains:

PATH: NETWORK CONFIGURATION > REGISTERED DOMAINS

1. Select the domain(s) that you want to remove.
2. Click **Delete**.

Registered Services

Add different servers for specific services that your organization uses internally or considers trustworthy to establish the network profile. Identifying trusted services in the network ensures detection of unauthorized applications and services.

You can add a maximum of 1,000 services, but add only trusted services to ensure accuracy of your network profile.

To add a registered service:

PATH: NETWORK CONFIGURATION > REGISTERED SERVICES

1. Select a service from the drop-down list.

TABLE 6-1. Service types

SERVICE	DESCRIPTION
DNS	The network server used as a DNS server
FTP	The network server used as an FTP server
HTTP Proxy	The network server used as an HTTP Proxy server
SMTP	The network server used as an SMTP server
SMTP Open Relay	The network server used as an SMTP Open Relay server
Software Update Server	The network server responsible for Windows Server Update Services (WSUS) or the server that performs remote deployment
Security Audit Server	The network server used to detect both vulnerabilities and insecure configurations

2. (Optional) Click **Analyze** to display a list of domains that you can add to the list.
3. (Optional) Specify a server name.

4. Specify an IP address.

   Note: IP address ranges cannot be specified.

5. Click **Add**.

To remove registered services:

PATH: NETWORK CONFIGURATION > REGISTERED SERVICES

1. Select the service(s) you want to delete.
2. Click **Delete**.

Network Configuration Replication

Network configuration settings include the monitored networks, registered domains, registered services, and detection exclusion list that you have configured. You can replicate these settings from one Threat Discovery Appliance to another by exporting the settings to a file and then importing the file to other Threat Discovery Appliances.

The default file name is cav.xml, which you can change to your preferred file name.

Note: To replicate Threat Discovery Appliance settings, in addition to network configuration settings, see *Configuration Backup and Restore* on page 8-3.

To replicate network configuration settings:

1. On the web console of the Threat Discovery Appliance containing settings to be replicated:
   a. Navigate to **Network Configuration > Export/Import Configuration**.
   b. Under **Export Configuration**, click **Export**. A message prompts you to open or save the cav.xml file.
   c. Click **Save**, browse to the target location of the file, and then click **Save**.

2. On the web console of the other Threat Discovery Appliance:
   a. Navigate to **Network Configuration > Export/Import Configuration**.
   b. Repeat steps 1b and 1c above to back up the current network configuration settings.
   c. Under **Import Configuration**, click **Browse**.
   d. Locate the cav.xml file and click **Open**.
   e. Click **Import**.

Detections

Detections establish filters and exclusions for the product's network detection features.

Threat Detections

Enable or disable the following features.

TABLE 6-2. Threat detection features

FEATURE	DESCRIPTION
Threat Detections	Detects both known and potential threats. Trend Micro enables this feature by default.
Outbreak Containment Services	Detects unknown malware that has the potential of starting an outbreak. Trend Micro enables this feature by default.
Block Traffic	Resets network connections of unknown malware when detected. Trend Micro disables this feature by default.

To configure threat detection:

PATH: DETECTIONS > THREAT DETECTIONS

1. Enable the **Enable threat detections** option.
2. Under **Threat Detections**, enable the second **Enable threat detections** option.
3. Under Outbreak Containment Services, select the **Enable outbreak detection and block traffic** option.
4. Click **Save**.

Detection Exclusion List

The Detection Exclusion List contains a list of IP addresses. Potential threats detected on any of the IP addresses will not be recorded in the logs.

Note: Known threats, including those detected by Application Filters, are recorded in the logs.

Outbreak Containment Services will also not block activities on the IP addresses that may lead to an outbreak. When configuring the exclusion list, ensure that you include only trusted IP addresses.

To configure the exclusion list for potential threats:

PATH: DETECTIONS > DETECTION EXCLUSION LIST

1. Select the **Potential Threat Detections** tab.
2. Select a **Protocol** from the drop-down list.
3. Specify a unique name for easy identification.
4. Specify an IP address or IP address range in the text field.
   - Use a dash to specify an IP address range, such as 192.168.1.0-192.168.1.255.
   - Use a slash to specify the subnet mask for IP addresses, such as 192.168.1.0/255.255.255.0 or 192.168.1.0/24.
5. Click **Add**.
6. To remove an entry from the list, select the entry and click **Delete**.

To configure the exclusion list for Outbreak Containment Services:

PATH: DETECTIONS > DETECTION EXCLUSION LIST

1. Select the **Outbreak Containment Services** tab.
2. Specify a unique name for easy identification.
3. Specify an IP address or IP address range in the text field.
   - Use a dash to specify an IP address range, such as 192.168.1.0-192.168.1.255.
   - Use a slash to specify the subnet mask for IP addresses, such as 192.168.1.0/255.255.255.0 or 192.168.1.0/24.
4. Click **Add**.
5. To remove an entry from the list, select the entry and click **Delete**.

Detected Files

The Detected Files screen contains a list of files with potential security risks. Threat Discovery Appliance tags these files as potential security risks/threats and makes a copy of the files for assessment.

The Detected Files screen displays the following information:

TABLE 6-3. Information on the Detected Files screen

LOG INFORMATION	DESCRIPTION
Date	The date and time the incident occurred To view details for a particular incident, click a link under **Date**. A new screen opens, with the details for the incident. For more information, see *Event Details* on page 7-28.
Protocol	Protocols such as HTTP, FTP, SMTP, and POP3
Direction	Indicates whether an incident happened inside the network or is an external attack
DstIP	IP address of the threat target
SrcIP	IP address of the source of the threat

TABLE 6-3. Information on the Detected Files screen (Continued)

LOG INFORMATION	DESCRIPTION
RiskType	The type of threat
File name	File name of the potential threat

Use the filter feature on the screen to search for specific files. You can save any of the files in the Detected Files screen and then submit them to Trend Micro for assessment.

To specify filter criteria:

PATH: DETECTIONS > DETECTED FILES

1. Click **Filter**. The Filter Criteria window opens.

   Note: The next items are optional. Specifying additional items will produce more targeted results, but being too specific might also produce no result.

2. Select a protocol from the list. Use the Control (Ctrl) key to select more than one protocol.
3. Type an IP address.
4. Select the traffic direction from the drop-down list.
5. Select a date range. Set the date range by typing a date or clicking the calendar icon.
6. Click **Filter**.

To save files:

PATH: DETECTIONS > DETECTED FILES

1. Select the files you want to save.
2. Click **Save detected file(s)**. Threat Discovery Appliance archives the files to a compressed file (.tgz).
3. Save the compressed file to your preferred location.

   WARNING! Do not open the compressed file as the files inside it might be infected.

Web Reputation

Threat Discovery Appliance leverages Trend Micro smart protection technology, a cloud-based infrastructure that determines the reputation of websites that users are attempting to access. Threat Discovery Appliance logs URLs that smart protection technology verifies to be fraudulent or known sources of threats. The product then uploads the logs to TMSP for report generation.

Note: Logs are not available in the Threat Discovery Appliance web console.

For detailed information about smart protection technology, see *Smart Protection Technology* on page 6-21.

Complementary to smart protection technology is Smart Feedback, an opt-in subscription to the threat feedback system that is part of Smart Protection Network™. Smart Feedback collects information about new or potential threats and then sends the information to Smart Protection Network so that Trend Micro can analyze and address these threats. Your participation in Smart Feedback means that you are authorizing Trend Micro to collect network information, which is kept in strict confidence. Information includes:

- This product's name and version
- URLs suspected to be fraudulent or possible sources of threats
- URLs associated with spam or possibly compromised
- Malware name for URLs that harbor malware

To configure web reputation settings:

PATH: DETECTIONS > WEB REPUTATION

1. Enable web reputation.
2. Select the smart protection source. Threat Discovery Appliance connects to the smart protection source to obtain web reputation data. For detailed information about the different smart protection sources, see *Smart Protection Technology* on page 6-21.
   - **Trend Micro Smart Protection Network:** Select this option if you do not plan to set up a Smart Protection Server. Internet connection is required to connect to this Trend Micro hosted service.
   - **Smart Protection Server:** Select this option if you have set up one or several Smart Protection Servers. Network connection is required to connect to this server.
3. If you choose **Smart Protection Server**:
   a. Type the Smart Protection Server's IP address.

      You can obtain the IP address from the Smart Protection Server console by navigating to **Smart Protection > Reputation Services > Web Reputation** tab. The IP address forms part of the URL listed in the screen.

   b. Click **Test Connection** to check if connection to the server can be established.

   c. Type a description for the server.

   d. Select whether to query the Smart Protection Network if the Smart Protection Server cannot determine a URL's reputation.

      The Smart Protection Server may not have reputation data for all URLs because it cannot replicate the entire Smart Protection Network data. When updated infrequently, the Smart Protection Server may also return outdated reputation data.

      Enabling this option improves the accuracy and relevance of the reputation data. However, it takes more time and bandwidth to obtain the data. Disabling this option has the opposite effects.

If you enable this option, do the following to optimize web reputation queries:

- On the Smart Protection Server's console, navigate to **Smart Protection > Reputation Services > Web Reputation tab > Advanced Settings** section. Disable **Use only local resources, do not send queries to Smart Protection Network**. This option prevents the Smart Protection Server from obtaining data from Smart Protection Network.
- Update the Smart Protection Server regularly.

You can disable this option if you do not want your organization's data to be transmitted externally.

e. If you have configured Proxy Settings for Threat Discovery Appliance and want to use these settings for Smart Protection Server connections, select **Connect through a proxy server**.

Note: If you disable proxy settings, Smart Protection Servers that connect through the proxy server will connect to Threat Discovery Appliance directly. Under the **Proxy Connection** column, the status is  **Proxy Unavailable**.

---

f. Click **Add**. The Smart Protection Server is added to the Smart Protection Server list.

g. Add more servers. You can add up to a maximum of 10 servers.

Tip: Trend Micro recommends adding multiple Smart Protection Servers for failover purposes. If Threat Discovery Appliance is unable to connect to a particular server, it tries connecting to the other servers.

---

h. If you have added several servers, Threat Discovery Appliance connects to these servers in the order in which they appear in the list. Use the arrows under the **Order** column to move servers up and down the list.

4. Choose to enable or disable Smart Feedback.
5. Click **Save**.

To manage the Smart Protection Server list:

PATH: DETECTIONS > WEB REPUTATION

1. To verify the connection status with a Smart Protection Server, click **Test Connection**.
2. To modify server settings:
   a. Click the server address.
   b. In the window that appears, modify the server's IP address, description, and settings.
   c. When you specify a new IP address, click **Test Connection** to confirm the connection.
   d. Click **OK**.
3. To remove a server from the list, click **Delete**.
4. Click **Save**.

Application Filters

Protect the network by enabling Application Filters. Application Filters provide valuable information to help you quickly identify security risks and prevent the spread of malicious code.

Enable detection for the following applications:

TABLE 6-4. Application types

APPLICATION	DESCRIPTION
Instant Messaging	A popular means of communicating and sharing information and files with contacts
P2P	Using peer-to-peer protocol to share files from one computer to another
Streaming Media	Audio-visual content that plays while downloading

To configure Application Filters settings:

PATH: DETECTIONS > APPLICATION FILTERS

1. Enable detection for **Instant Messaging**.
   a. Select the **Instant Messaging** check box.
   b. Select the specific protocols for detection.

   Tip: Use the CTRL key to select one or multiple protocol types.

   c. Move the selected protocol under **Selected Instant Messaging protocols**.
2. Enable detection for **P2P Traffic**.
   a. Select the **P2P Traffic** check box.
   b. Select the specific protocols for detection.

   Tip: Use the CTRL key to select one or multiple protocol types.

   c. Move the selected protocol under **Selected Peer-to-Peer applications**.
3. Enable detection for **Streaming Media**.
   a. Select the **Streaming Media** check box.
   b. Select the specific protocols for detection.

   Tip: Use the CTRL key to select one or multiple protocol types.

   c. Move the selected protocol under **Selected streaming media applications**.
4. Click **Save**.

Client Identification

When Threat Discovery Appliance detects a threat, it logs the IP address in use on the affected endpoint. If IP addresses are dynamically assigned in your organization, consider enabling client identification.

Client identification works by determining the NetBIOS name, DNS domain name, and Active Directory domain and account name used on the affected endpoint at the time of threat detection. These names display on the Product Summary screen and in the Event Details screen.

- To determine the NetBIOS name, Threat Discovery Appliance connects to the endpoint through port 137.

  Note: Security software residing on the endpoint may notify the user of the connection on port 137. If the notification can be disabled, consider disabling it to prevent any unnecessary disruptions to users.

- To determine the DNS domain name, Threat Discovery Appliance queries the DNS server.
- To determine the Active Directory domain and account name, Threat Discovery Appliance analyzes the Active Directory logon traffic.

To configure client identification settings:

PATH: DETECTIONS > CLIENT IDENTIFICATION

1. Enable identification of the following:
   - NetBIOS names
   - DNS domain names
   - Active Directory domain and account names
2. Click **Save**.
3. To disable identification, clear any of the check boxes and then click **Save**.

Threshold Settings

A security risk meter displaying on the Summary screen and on the upper left-hand corner of the main menu indicates the network's overall risk level based on the number of potential security risk events detected by Threat Discovery Appliance.

Note: The security risk meter only counts potential security risk events, not known security risks or threats.

Use threshold settings to define the number of events considered a low or critical risk.

- **Critical risk:** Any number that signifies a need for you to constantly monitor your network or take preventive or corrective action. This can be any value you set. Threat Discovery Appliance considers anything lower than this value as low risk.
- **Low risk:** Any number that signifies a need for monitoring the network. This can be any value you set. Threat Discovery Appliance considers anything lower than this value as normal network behavior.

To configure threshold settings:

PATH: SUMMARY

1. In the **Detection Status** tab, click **Settings**.
2. In the **Low risk** setting, specify the minimum number of potential security risk events per time unit considered a low risk. The default value for Low Risk is 20 events for every minute.
3. In the **Critical risk** setting, select the minimum number of potential security risk events for every time unit considered a critical risk. The default value for Critical Risk is 100 events for every minute.

Tip: Trend Micro recommends adjusting the default values according to the size of your network.

4. Click **Save**.

Security Compliance

Security Compliance is a separately licensed feature in Threat Discovery Appliance that extracts meaningful content from various file formats and archives. Security Compliance then checks whether the content contains information regulated by compliance rules. Threat Discovery Appliance logs violations to compliance rules and then uploads the logs to TMSP.

Note: Logs are not available in the Threat Discovery Appliance web console.

Compliance rules are contained in templates. Threat Discovery Appliance comes with a set of predefined templates for specific industries and regulations, such as:

- Payment Card Industry Data Security Standard (PCI-DSS)
- California Security Breach Information Act (SB-1386)
- Health Insurance Portability and Accountability Act (HIPAA)
- Financial Services Modernization Act (GLBA)
- US Personally Identifiable Information Act (US PII)

You can import custom templates containing compliance rules not covered in predefined templates. Contact Trend Micro for information about available custom templates.

Before enabling Security Compliance, ensure that you have activated its license. For more information about activation, see *Licenses and Activation Codes* on page 5-9.

To use Security Compliance:

PATH: SECURITY COMPLIANCE

1. Enable Security Compliance.
2. To import a custom template:
   a. Click **Import Template**.
   b. Browse to the location of the custom template.
   c. Click **Import**.
3. Click **Save**.

Integration with Trend Micro Products and Services

Threat Discovery Appliance integrates with the Trend Micro products and services listed in *Table 6-5*. For seamless integration, ensure that the products run the required or recommended versions.

TABLE 6-5. Trend Micro products and services that integrate with Threat Discovery Appliance

PRODUCT/ SERVICE	DESCRIPTION	VERSION
Threat Mitigator	Receives mitigation requests from Threat Discovery Appliance after a threat is detected. Threat Mitigator then notifies Threat Management Agent installed on an endpoint to run a mitigation task. For details, see *Mitigation Devices* on page 6-27. **Note:** Threat Mitigator is part of Threat Management Services. For details, see *About Trend Micro Threat Management Services* on page 1-2.	• 2.6 (recommended) • 2.x (minimum)

TABLE 6-5. Trend Micro products and services that integrate with Threat Discovery Appliance (Continued)

PRODUCT/ SERVICE	DESCRIPTION	VERSION
Threat Management Services Portal (TMSP)	Receives logs and data from Threat Discovery Appliance, and then uses them to generate reports containing security threats and suspicious network activities, and Trend Micro recommended actions to prevent or address them. For details, see *Threat Management Services Portal* on page 6-24. **Note:** TMSP is part of Threat Management Services. For details, see *About Trend Micro Threat Management Services* on page 1-2.	• 2.6 (for the on-premise edition of TMSP) • Not applicable for the Trend Micro hosted service
Smart Protection Network	Provides the Web Reputation Service, which determines the reputation of websites that users are attempting to access. Smart Protection Network is hosted by Trend Micro. For details, see *Smart Protection Technology* on page 6-21.	Not applicable
Smart Protection Server	Provides the same Web Reputation Service offered by Smart Protection Network. Smart Protection Server is intended to localize the service to the corporate network to optimize efficiency. For details, see *Smart Protection Technology* on page 6-21.	2.0

TABLE 6-5. Trend Micro products and services that integrate with Threat Discovery Appliance (Continued)

PRODUCT/ SERVICE	DESCRIPTION	VERSION
Network VirusWall Enforcer	Regulates network access based on the security posture of endpoints. For details, see *Mitigation Devices* on page 6-27.	• 3.0 with Patch 1 • 2.0 Service Pack 1 with Patch 1
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 6-29.	• 5.5 • 5.0

Smart Protection Technology

Trend Micro smart protection technology is a next-generation, in-the-cloud protection solution providing File and Web Reputation Services. By leveraging the Web Reputation Service, Threat Discovery Appliance can obtain reputation data for websites that users are attempting to access. Threat Discovery Appliance logs URLs that smart protection technology verifies to be fraudulent or known sources of threats and then uploads the logs to TMSP for report generation.

Note: Threat Discovery Appliance does not use the File Reputation Service that is part of smart protection technology.

Reputation services are delivered through smart protection sources, namely, **Trend Micro Smart Protection Network** and **Smart Protection Server**. These two sources provide the same reputation services and can be leveraged individually or in combination. The following table provides a comparison between these sources.

TABLE 6-6. 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.	Trend Micro product administrators install and manage this server.
Connection protocol	HTTPS	HTTP
Usage	Use if you do not plan to install Smart Protection Server. To configure Smart Protection Network as source, see *Web Reputation* on page 6-11.	Use as primary source and the Smart Protection Network as an alternative source. For guidelines in setting up Smart Protection Server and configuring it as source, see *Setting Up Smart Protection Server* on page 6-23.

Setting Up Smart Protection Server

Perform the following tasks to set up a Smart Protection Server:

1. Install Smart Protection Server on a VMware ESX/ESXi server.

   Installation reminders and recommendations:

   - For information on the Smart Protection Server versions compatible with Threat Discovery Appliance, see *Integration with Trend Micro Products and Services* on page 6-19.
   - For installation instructions and requirements, refer to the *Installation and Upgrade Guide for Trend Micro Smart Protection Server.*
   - Smart Protection Server, Threat Discovery Appliance, and the VMware ESX/ESXi server (which hosts the Smart Protection Server) require unique IP addresses. Check the IP addresses of the VMware ESX/ESXi server and Threat Discovery Appliance 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 Mitigator), you can use the same server for Threat Discovery Appliance. While several Trend Micro products can send queries simultaneously, the Smart Protection Server may become overloaded as the volume of queries increases. Ensure that the Smart Protection Server can handle queries coming from different products. Contact your support provider for sizing guidelines and recommendations.
   - Trend Micro recommends installing multiple Smart Protection Servers for failover purposes. Threat Discovery Appliance checks The Smart Protection Server list configured in the web console to determine which server to connect to first, and the alternative servers if the first server is unavailable.

2. Configure Smart Protection Server settings from the Threat Discovery Appliance console. For details, see *Web Reputation* on page 6-11, starting in step 3.

Threat Management Services Portal

Threat Management Services Portal (TMSP) receives logs and data from registered products and then issues targeted reports to product users. Register Threat Discovery Appliance 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 Discovery Appliance by:

- Analyzing logs and data coming from Threat Discovery Appliance, including:
  - Detection logs
  - Application filter logs
  - URL filtering logs
  - Security Compliance logs
  - Network configuration data, including monitored networks, registered domains, and registered services. TMSP displays network configuration data in reports and in various places in the TMSP administrative console.

  Note: URL Filtering and Security Compliance logs are not available in the Threat Discovery Appliance web console.

- Generating threat reports

  Reports contain security threats and suspicious network activities, and Trend Micro recommended actions to prevent or address them. Daily administrative reports enable IT administrators to track the status of threats, while weekly and monthly executive reports keep executives informed about the overall security posture of the organization.

Threat Discovery Appliance sends heartbeat messages to TMSP periodically. A heartbeat message informs TMSP that Threat Discovery Appliance is up and running and can therefore send logs.

Threat Discovery Appliance can use proxy server settings configured on the Proxy Settings screen to connect to TMSP.

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 Discovery Appliance, see *Integration with Trend Micro Products and Services* on page 6-19.

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

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

To configure TMSP settings:

PATH: THREAT MANAGEMENT SERVICES PORTAL

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

   Note: Disabling this option unregisters Threat Discovery Appliance from TMSP. If you disable this option:

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

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

2. Specify the log server for TMSP.
   - If you have TMSP as a hosted service, type the IP address or host name.
   - If you have TMSP as an on-premise application, type the IP address.
3. Select the protocol. You can select either **SSH** or **SSL**.

- If you have set up a firewall, configure the firewall to allow traffic from Threat Discovery Appliance to TMSP through port 443 (if you selected SSL) or port 22 (if you selected SSH).
- If you selected SSH and have set up Microsoft ISA Server, configure the tunnel port ranges on the ISA server to allow traffic from Threat Discovery Appliance to TMSP through port 22.

4. Specify how often to send logs to TMSP.
5. Specify the status server for TMSP.
   - If you have TMSP as a hosted service, type the IP address or host name.
   - If you have TMSP as an on-premise application, type the IP address.

Note: The status server receives the following information from Threat Discovery Appliance:

- Heartbeat message. Threat Discovery Appliance sends a heartbeat message at regular intervals to inform TMSP that it is up and running.

- Outbreak Containment Services logs

---

6. Type the server authentication credentials (user name and password). TMSP authenticates Threat Discovery Appliance using these credentials and then proceeds to accept logs and data.
7. Type the registration email address.

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

---

8. If you have configured Proxy Settings for Threat Discovery Appliance and want to use these settings for TMSP connections, select **Connect through a proxy server**.
9. To check whether Threat Discovery Appliance can connect to TMSP based on the settings you configured, click **Test Connection**.
10. Click **Save** if the test connection is successful.

Mitigation Devices

Mitigation devices receive threat information gathered by Threat Discovery Appliance. These devices work with an agent program installed on an endpoint to address and resolve threats. A device with the network access control function may prevent the endpoint from accessing the network until the endpoint is free of threats.

You can register Threat Discovery Appliance to a maximum of 20 mitigation devices. For information on the device versions compatible with Threat Discovery Appliance, see *Integration with Trend Micro Products and Services* on page 6-19.

To register to mitigation devices:

PATH: MITIGATION > MITIGATION SETTINGS

1. Under **Mitigation Settings**, type the mitigation device **Server name or IP address**.
2. Type a **Description** for the device.
3. Specify **IP address ranges**.

> **Note:** To save network bandwidth, specify IP address ranges for each mitigation device. Threat Discovery Appliance only sends mitigation tasks for specific IP addresses to the mitigation device. If the IP address range is empty, all mitigation requests will be sent to the mitigation device.

4. Click **Register**. The Cleanup Settings screen appears.
5. Select the types of security risks/threats to send to the mitigation device.
6. Click **Apply**.

To unregister from mitigation devices:

PATH: MITIGATION > MITIGATION SETTINGS

1. Select the mitigation devices to unregister from.
2. Click **Delete**. The device is removed from the list. This task also triggers the mitigation device to remove Threat Discovery Appliance from its list of data sources.

Mitigation Exclusion List

Exclude IP addresses from mitigation actions. Threat Discovery Appliance still scans these IP addresses but does not send mitigation requests to the mitigation device if threats are found.

Before configuring the mitigation exclusion list, ensure that you have registered Threat Discovery Appliance to at least one mitigation device. For details, see *Mitigation Devices* on page 6-27.

You can add a maximum of 100 entries to the list.

To configure the mitigation exclusion list:

PATH: MITIGATION > MITIGATION EXCLUSION LIST

1. Type a name for the exclusion. Specify a meaningful name for easy identification, such as "Lab Computers".
2. Specify an IP address or IP address range for exclusion from mitigation actions. For example, 192.1.1.1-192.253.253.253.
3. Click **Add**.
4. To remove an entry from the list, select the entry and click **Delete**.

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 Discovery Appliance, see *Integration with Trend Micro Products and Services* on page 6-19.

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

Control Manager Components

Table 6-7 lists the components that make up Control Manager.

TABLE 6-7. 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 Discovery Appliance that allows Control Manager to manage the product. The agent receives commands from the Control Manager server, and then applies them to Threat Discovery Appliance. 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 Discovery Appliance, and status reports from Threat Discovery Appliance to the Control Manager server all pass through this component.

TABLE 6-7. Control Manager components (Continued)

COMPONENT	DESCRIPTION
Entity	A representation of a managed product (such as Threat Discovery Appliance) 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 Discovery Appliance console to perform the following:

- Check the connection between Threat Discovery Appliance 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 Discovery Appliance can register to a Control Manager server

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

To register Threat Discovery Appliance to Control Manager:

PATH: ADMINISTRATION > CONTROL MANAGER SETTINGS

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

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

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 **User name** and **Password** fields.

3. 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 Discovery Appliance 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.

---

4. If you have configured Proxy Settings for Threat Discovery Appliance and want to use these settings for Control Manager connections, select **Connect through a proxy server**.
5. To check whether Threat Discovery Appliance 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 Discovery Appliance 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. Select **Managed Products** from the list.
4. Check if the Threat Discovery Appliance icon displays.

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 Discovery Appliance) 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 Discovery Appliance, click **Unregister** and then register Threat Discovery Appliance to the other server.

Chapter 7

Viewing and Analyzing Information

This chapter includes information about identifying security risks and evaluating practices to protect against security risks.

The topics discussed in this chapter are:

Status Indicators

Threat Discovery Appliance displays status indicators on the upper left-hand corner of the main menu.

FIGURE 7-1. Status indicators

If Threat Discovery Appliance can retrieve information about hardware resources, appliance health will also display.

FIGURE 7-2. Status indicators showing appliance health information

Risk Meter

Risk Meter indicates the network's overall risk level based on the number of potential security risk events detected by Threat Discovery Appliance. The Risk Meter status indicates the following:

TABLE 7-1. Risk meter status

STATUS	DESCRIPTION
Normal	A green indicator signifies that there are minimal or no risks that need to be monitored or no actions needs to be performed.
Low risk	A yellow indicator signifies that there is a need to monitor the network.
Critical risk	A red indicator signifies that there is a need to constantly monitor the network and take preventive or corrective action.

You can configure the number of events considered a low or critical risk from the Threshold Settings screen. For details, see *Threshold Settings* on page 6-17.

Appliance Health

Appliance Health displays the status of hardware resources for the product.

TABLE 7-2. Appliance health status

STATUS	DESCRIPTION
Normal	A green indicator signifies that the appliance temperature is normal.
Warning	A yellow indicator signifies that the appliance or CPU temperature is between 90-100% of the limit. Check the temperature or ensure that the fan is working.
Critical	A red indicator signifies that the appliance or CPU temperature is 100% or higher than the safe range. Check the appliance temperature or ensure that the fan is working.

Network Flow

The network flow status indicates the following:

TABLE 7-3. Network flow status

STATUS	DESCRIPTION
Normal	A green indicator signifies that Threat Discovery Appliance is able to handle traffic flowing through the network.
Critical	A red indicator signifies that the network flow exceeds Threat Discovery Appliance capacity. Verify the capacity of the switch mirror port and the network traffic.

Product Summary

The Summary screen displays when you open the product console or click **Summary** on the main menu. The Summary screen has three sections:

- The **Reminders** section on top of the screen displays only when there are important reminders regarding the product license and database.
- The **Detection Status** tab provides information about the latest detected threats and system events, such as component updates.
- The **System Status** tab shows CPU and memory usage information.

The Summary screen automatically resets every 10 seconds. Click **Refresh** to display the latest information on the screen.

Reminders

Important reminders about the product license and database display in this section of the Summary screen.

FIGURE 7-3. Reminders section on top of the Summary screen

TABLE 7-4. Events that trigger reminders

EVENT	DETAILS
License expiration	Reminders display when a license is about to expire or has expired. For details, see *Fully Licensed and Evaluation Versions* on page 5-9.
Database corruption	A reminder displays when the product database becomes corrupted. Repair the corrupted database files immediately from the Log Maintenance screen. For details, see *Log Maintenance* on page 8-2.

Detection Status - Detections in Past 24 Hours

This section of the Summary screen displays the incidents that Threat Discovery Appliance detected over the past 24 hours.

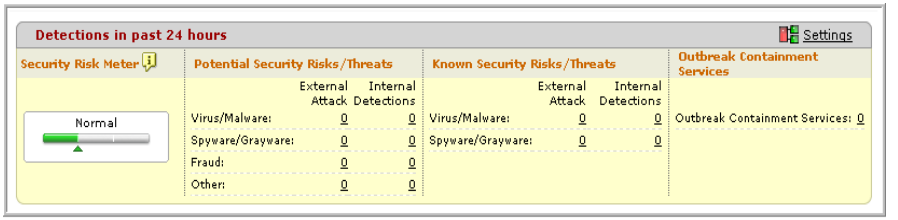


FIGURE 7-4. Detections in past 24 hours section

TABLE 7-5. Information in the Detections in past 24 hours section

INFORMATION	DESCRIPTION
Security Risk Meter	View the network's overall risk level based on the number of potential security risk events detected by Threat Discovery Appliance. The Risk Meter status indicates the following: • **Normal:** A green indicator signifies that there are minimal or no risks that need to be monitored or no actions needs to be performed. • **Low risk:** A yellow indicator signifies that there is a need to monitor the network. • **Critical risk:** A red indicator signifies that there is a need to constantly monitor the network and take preventive or corrective action. You can configure the number of events considered a low or critical risk from the Threshold Settings screen. For details, see *Threshold Settings* on page 6-17.
Potential Security Risks/Threats	View the number of potential security risks/threats. This means certain actions or events alerted Threat Discovery Appliance of a possible security risk/threat originating from within or outside the network. Click the number of detections for details on the incident.

TABLE 7-5. Information in the Detections in past 24 hours section (Continued)

INFORMATION	DESCRIPTION
Known Security Risks/Threats	View the number of known security risks/threats originating from within or outside the network. Click the number of detections for details on the incident.
Outbreak Containment Services	View the number of potential malware activities that might cause an outbreak. Click the number of events for additional information.

Detection Status - Recent Alerts

This section of the Summary screen lists the most recent incidents detected by the product.

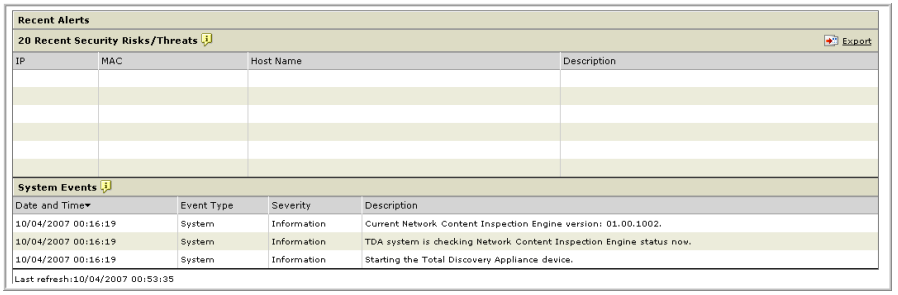


FIGURE 7-5. Recent Alerts section

TABLE 7-6. Recent alerts

ALERT	DESCRIPTION
20 Recent Security Risks/Threats	Contents in this alert are not limited to the past 24 hours. • View the most recent potential and known threats with "High" severity rating. • The IP address, MAC address, host name, and description of the security risks/threats display. • Click a link under **IP Address** or **Mac Address**. An **Event Log** table displays. Click a link under **Date**. A new screen opens, providing details for the event. For more information, see *Event Details* on page 7-28. • Click the **Export** button to export additional security risks/threats details to a .csv file. • The **Description** column displays information about known and potential threats.
System Events in Past 24 Hours	View system events (such as when the product restarts or encounters problems) and component updates.

System Status

Monitor system performance from the **System Status** screen.

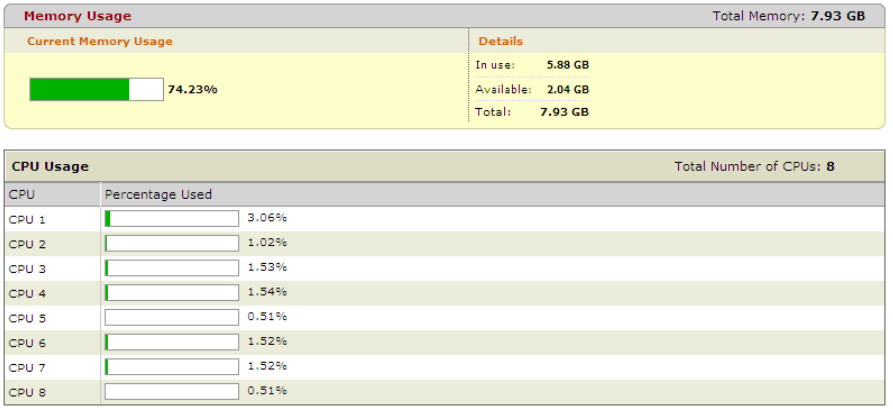


FIGURE 7-6. System Status screen

TABLE 7-7. System status information

INFORMATION	DESCRIPTION
Memory Usage	This section shows both the percentage of currently used memory and actual available memory. The indicator color is green if memory usage is 89% or less. It turns yellow when memory usage is between 90% and 99%, and red if 100%. Memory usage information is also available on the Preconfiguration Console. For details, see *Preconfiguration Menu: Device Information and Status* on page 4-6.
CPU Usage	This section shows the percentage of CPU consumption for each CPU used by Threat Discovery Appliance. The indicator color is green if CPU usage is 89% or less. It turns yellow when CPU usage is between 90% and 99%, and red if 100%.

Notifications

You can configure Threat Discovery Appliance to send notifications for certain events that occur in the network.

These notifications are delivered to the intended recipients through email, in plain text format. To configure email settings, see *Delivery Options for Notifications* on page 7-17.

Threshold-based Notifications

These notifications are triggered when the configured threshold for certain events is met. Notifications are sent immediately.

TABLE 7-8. Events that trigger threshold-based notifications

EVENT	DESCRIPTION
Detection of potential security risks	The notification received when outbound or inbound traffic meets the threshold you set or when Threat Discovery Appliance detects potential security risks
Detection of known security risks	The notification received when outbound or inbound traffic meets the threshold you set or when Threat Discovery Appliance detects known security risks
Detection of high risk clients	The notification received when the number of detections for every IP Address meets the threshold
High network traffic usage	The notification received when your network traffic exceeds the normal traffic pattern

Real-time Notifications

Notifications are triggered when events that require immediate attention occur. Threat Discovery Appliance sends notifications immediately or at specified intervals.

TABLE 7-9. Events that trigger real-time notifications

EVENT	DESCRIPTION
Detection of critical security risks	The notification received when critical security risks are detected

To configure notification settings:

PATH: NOTIFICATIONS > NOTIFICATION SETTINGS

1. Click a hyperlink under **Threshold-based Notifications** or **Real-time Notifications**.
2. Configure settings in the new window that opens. See the following topics for details:
   - Threshold-based Notification for Potential Security Risks
   - Threshold-based Notification for Known Security Risks
   - Threshold-based Notification for High Risk Clients
   - Threshold-based Notification for High Network Traffic Usage
   - Real-time Notification for Critical Security Risks

Threshold-based Notification for Potential Security Risks

Threat Discovery Appliance can send an email when it detects potential security risks. Use the Potential Security Risk Notification screen to configure the notifications sent to the designated individuals.

To configure notifications for detection of potential security risks:

PATH: NOTIFICATIONS > NOTIFICATION SETTINGS > DETECTION OF POTENTIAL SECURITY RISKS

1. Select **Notify administrator**.
2. Under **Notify if number of detections for**, configure the number of detections that triggers an alert for the following types of logs:
   - Outbound traffic means detections from monitored networks
   - Inbound traffic means detections from outside the network
3. Specify the number of hours or minutes within which Threat Discovery Appliance must detect the specified number of events to trigger an alert.

   Tip: Trend Micro recommends using the default settings.

4. Under **Detect the following**, select which security risks would trigger the notification.
5. Click **Save**.

To disable notifications:

PATH: NOTIFICATIONS > NOTIFICATION SETTINGS > DETECTION OF POTENTIAL SECURITY RISKS

1. Clear **Notify administrator**.
2. Click **Save**.

Threshold-based Notification for Known Security Risks

Threat Discovery Appliance can send an email when it detects known security risks. Use the Known Security Risk Notifications screen to configure the notifications sent to the designated individuals.

To configure notifications for detection of known security risks:

PATH: NOTIFICATIONS > NOTIFICATION SETTINGS > DETECTION OF KNOWN SECURITY RISKS

1. Select **Notify administrator**.
2. Under **Notify if number of detections for**, configure the number of detections which triggers an alert for the following types of logs:
   - **Outbound traffic** means detections from monitored networks
   - **Inbound traffic** means detections from outside the network
3. Specify the number of hours or minutes within which Threat Discovery Appliance must detect the specified number of log records.

   Tip: Trend Micro recommends using the default settings.

4. Under **Detect the following**, select which security risks would trigger the notification.
5. Click **Save**.

To disable notifications:

PATH: NOTIFICATIONS > NOTIFICATION SETTINGS > DETECTION OF KNOWN SECURITY RISKS

1. Clear **Notify administrator**.
2. Click **Save**.

Threshold-based Notification for High Risk Clients

Threat Discovery Appliance can send an email when it detects high risk clients. Threat Discovery Appliance classifies these clients as high risk when they exceed the specified number of detections. Use the High Risk Client Notification screen to configure the notifications sent to the designated individuals. These notifications contain information that can help you determine why a client is reporting a high number of detections and how to resolve this issue before it becomes the source of an outbreak.

To configure notifications for detection of high risk clients:

PATH: NOTIFICATIONS > NOTIFICATION SETTINGS > DETECTION OF HIGH RISK CLIENTS

1. Select **Notify administrator**.
2. Under **Notify if number of detections per IP address**, configure the number of detections per IP address that triggers an alert.
3. Specify the number of hours or minutes within which Threat Discovery Appliance must detect the specified number of log records.

> **Tip:** Trend Micro recommends using the default settings.

4. Click **Save**.

To disable notifications:

PATH: NOTIFICATIONS > NOTIFICATION SETTINGS > DETECTION OF HIGH RISK CLIENTS

1. Clear **Notify administrator**.
2. Click **Save**.

Threshold-based Notification for High Network Traffic Usage

Threat Discovery Appliance can send an email when network traffic usage exceeds a certain threshold, which might happen if there is an external attack. Use the High Traffic Usage Notification screen to configure notifications sent to designated individuals.

The data on the screen resets if the product restarts or shuts down.

Note: The numbers 0 to 23 on the horizontal axis of the **Normal Traffic Pattern** graph indicate the amount of time that passed since Threat Discovery Appliance scanned and produced the graph. They do not signify the time Threat Discovery Appliance scanned the network. 0 indicates the current size of scanned traffic, while 4 indicates the size 4 hours ago.

To configure notifications for detection of high network traffic usage:

PATH: NOTIFICATIONS > NOTIFICATION SETTINGS > HIGH NETWORK TRAFFIC USAGE

1. Select **Notify administrator**.
2. Click **Auto-Detect** for Threat Discovery Appliance to define the normal traffic threshold or manually identify the traffic threshold at certain hours of the day.
   - The traffic threshold default unit is 1GB.
   - The amount of network traffic is rounded to the nearest whole number. For example, 1.2GB displays as 2GB and 2.6GB displays as 3GB.
3. Click **Save**.

To disable notifications:

PATH: NOTIFICATIONS > NOTIFICATION SETTINGS > HIGH NETWORK TRAFFIC USAGE

1. Clear **Notify administrator**.
2. Click **Save**.

Real-time Notification for Critical Security Risks

Threat Discovery Appliance triggers real-time notifications as soon as it detects critical security risks in the network to allow you to take immediate action. You can configure the product to send these notifications immediately or at specified intervals.

By default, the product will send notifications for critical security risks detected on all endpoints. Use the exclusion list for endpoints that you do not want to be notified about.

To configure notifications for critical security risks:

PATH: NOTIFICATIONS > NOTIFICATION SETTINGS > DETECTIONS OF CRITICAL SECURITY RISKS

1. Select the option to enable real-time notifications.
2. Under **Potential Security Risks**, select the option to send a notification when a high-severity security risk is detected.
3. Under **Known Security Risks**, select the option to send a notification when virus/malware or spyware/grayware is detected.
4. Specify the email-sending interval in number of minutes, hours, or days.

   For each endpoint, Threat Discovery Appliance aggregates notifications triggered within the time interval and sends them as one email message when the time interval elapses. For example, if critical security risks were detected on 12 endpoints, Threat Discovery Appliance sends 12 email messages. Each message contains a list of critical security risks detected in the endpoint within the time interval.
5. Click **Save**.

To configure the exclusion list:

PATH: NOTIFICATIONS > NOTIFICATION SETTINGS > DETECTIONS OF CRITICAL SECURITY RISKS

1. Click the **Exclusion List** tab.
2. Type a descriptive name for the exclusion list.
3. Type the IP address/range of endpoints to be excluded from real-time notifications.
4. Click **Add**.

Note: You can add up to 100 exclusion lists.

5. To remove an exclusion list, mark the check box before the exclusion list and then click **Delete**.
6. Click **Save**.

Delivery Options for Notifications

Use the Delivery Options screen to configure the default sender, recipients, and settings of the notifications sent to designated individuals for specific events in the network. Configure these settings for the recipients to receive the necessary information to prevent or contain an outbreak.

To configure the delivery options:

PATH: NOTIFICATIONS > DELIVERY OPTIONS

1. Under **Notification recipient**, type the recipient. Use a semicolon ";" to separate multiple addresses.
2. Under **Sender's email address,** type the sender. You can only add one valid email address.
3. Type the SMTP server name or IP address and port.
4. If the SMTP server requires authentication, specify the user name and password for the SMTP server. Ensure that you add the Threat Discovery Appliance IP address to the SMTP relay list.
5. Specify the maximum number of notifications and the number of minutes to check the mail queue.

Tip: Trend Micro recommends using the default settings.

6. Click **Save**.

Reports

Threat Discovery Appliance reports provide an online collection of figures about incidents or detections, clients, and network traffic. Reports display in a variety of formats, including tables, bar, line, and pie graphs. On the Reports screen on the product console, there are three tabs containing the following reports:

- Reports: Number of Incidents
- Reports: High Risk Clients
- Reports: Network Traffic

Users can receive email messages reminding them about the latest reports available on the product console. For details, see *Reports: Delivery Settings* on page 7-23.

Reports: Number of Incidents

PATH: REPORTS > NUMBER OF INCIDENTS

The **Number of Incidents** tab displays daily reports on security risks detected in the network and separates the incidents by protocol, detection type, and time of day. You can quickly view and print these bar and pie graph reports.

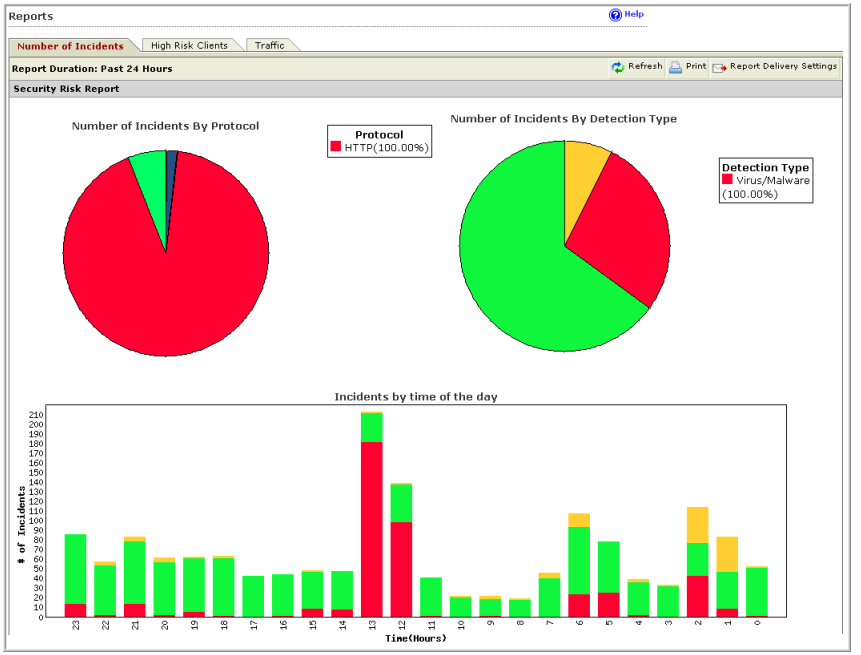


FIGURE 7-7. Number of Incidents report

Number of Incidents by Protocol

The **Number of Incidents by Protocol** displays the protocols (such as HTTP, FTP, SMTP, POP3, IRC, and IM) and the percentage of its occurrence within the past 24 hours. These protocols and percentages are seen in the pie graph and legend list.

Number of Incidents by Detection Type

The **Number of Incidents by Detection Type** displays the detection types (such as virus/malware, spyware/grayware, and fraud) and the percentage of its occurrence within the past 24 hours. These detection types and percentages are seen in the pie graph and legend list.

Number of Incidents by Time of Day

The numbers 0 to 23 on the horizontal axis of the **Number of Incidents by Time of Day** graph indicate the amount of time that passed since Threat Discovery Appliance scanned and produced the graph. They do not signify the time Threat Discovery Appliance scanned the network. 0 indicates the current number of incidents, while 4 indicates the number of incidents 4 hours ago.

Reports: High Risk Clients

PATH: REPORTS > HIGH RISK CLIENTS

The **High Risk Client** tab displays daily reports of the riskiest clients, top propagation source, and top matched rule.

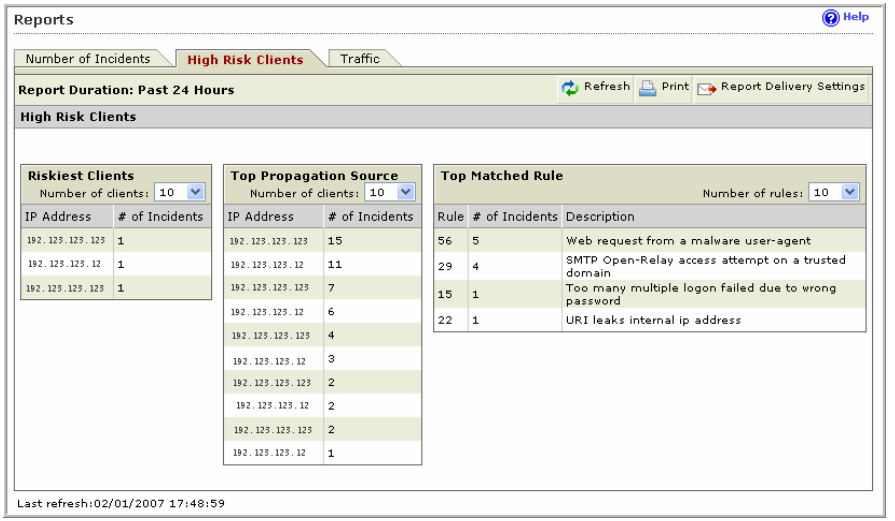


FIGURE 7-8. High Risk Clients report

Riskiest Clients

The **Riskiest Clients** table displays the IP addresses in the monitored network with the most number of incidents or attacks.

Top Propagation Source

The **Top Propagation Source** table displays the IP addresses in the monitored network propagating the most number of incidents.

Top Matched Rule

The **Top Matched Rule** table displays the triggered rules, the number of incidents, and rule descriptions that have the most number of incidents. Triggered rules are established by Trend Micro using the Network Content Inspection Engine and Network Content Correlation Engine. Trend Micro continuously updates the Network Content Inspection Engine and Network Content Correlation Pattern and rules.

Reports: Network Traffic

PATH: REPORTS > TRAFFIC

The **Traffic** tab displays the daily traffic scanned per hour of the day, traffic scanned per protocol (such as HTTP and SMTP), and file types that go through the network. The data on the tables resets if the product restarts or shuts down.

FIGURE 7-9. Traffic report

Total Traffic (in GB) Scanned

The numbers 0 to 23 on the horizontal axis of the **Total Traffic (in GB) Scanned** graph indicate the amount of time that passed since Threat Discovery Appliance scanned and produced the graph. They do not signify the time Threat Discovery Appliance scanned the network. 0 indicates the current size of scanned traffic, while 4 indicates the size 4 hours ago.

Traffic (in GB) Scanned Per Protocol

The **Traffic (in GB) Scanned per Protocol** graphs display the network traffic (for the HTTP, SMTP, and other protocols) scanned for the past 24 hours.

Traffic by File Types (Number of Files)

The **Traffic by File Types (Number of Files)** table displays the types of files either sent or received from the network for the past 7 days.

Reports: Delivery Settings

Use the report delivery settings to receive email messages reminding you about reports available on the product console. Email messages are sent daily.

To receive email messages:

PATH: REPORTS > REPORT DELIVERY SETTINGS

1. Select **Send email notifications everyday at 5:00 AM**.
2. Click **Save**.

To stop receiving email messages:

PATH: REPORTS > REPORT DELIVERY SETTINGS

1. Clear **Send email notifications everyday at 5:00 AM**.
2. Click **Save**.

Logs

Threat Discovery Appliance keeps comprehensive logs about security risk incidents, events, and updates. The log contains all the results of the assessment and the status of computers. These log entries are stored on the product's hard disk.

You can store these logs in the Trend Micro Control Manager database or a Syslog server. You can also perform log queries to gather information and create reports from the log database.

TABLE 7-10. Log types

TYPE	DESCRIPTION
Detection Logs	Information on potential and known threats, external attacks, and internal detections.
Application Filter Logs	Information on the application filter activities.
System Logs	Summaries of events regarding the product, such as component updates and product restarts.

Detection Logs

Each time Threat Discovery Appliance scans the network and detects a threat, it stores the results of the assessment and the status of the scanned computers on the Detection Log. Use this screen to obtain information from these logs.

If you registered Threat Discovery Appliance to Control Manager, Control Manager stores the scan results received from Threat Discovery Appliance.

To query detection logs:

PATH: LOGS > DETECTION LOG QUERY

1. Select the **Protocol** type. Select more than one protocol by pressing SHIFT and the protocols or CTRL and the selected protocols.
2. Select the **Traffic** direction. Select from **Internal attacks**, **External detections**, or both.

3. Select the **Detection** type. Select items from **Potential security risks**, **Known security risks**, **Files not scanned**, and **Outbreak Containment Services**.

   Note: The **Constraint met** option under **Files not scanned** refers to the files that exceeded the file scanning limitation.

4. Select **Mitigation** type of endpoint computers. Select from **Mitigated** and/or **Un-Mitigated**.
5. Select the **Severity** of the security risk. Select from **High**, **Medium**, **Low**, and/or **Informational** logs.
6. Select the **Group name**.

TABLE 7-11. Group name options

OPTION	DESCRIPTION
Group name	Select from one of the group names in the list
Specify group name	Type the specific group name, including deleted group names
Removed group	Select this option if the group name is not available in the list and you are unable to remember the exact name or if the group name has been deleted
No group	Select this option for those that do not fall under any of the other categories

7. Select the **Network Zone**. Select from **Trusted**, **Untrusted**, and/or **No network zone**.
8. Specify the **Date range** or click the calendar icon and select the date you want.
9. Select the IP address(es). Select from **All**, **IP address**, or a range of IP addresses.

10. (Optional) Type the **MAC Address, Computer Name**, and **Active Directory Domain Name** and **Account**.

    Note: Computer name and Active Directory domain name and account queries support partial matching.

11. Enable **Show executive logs** to view only logs with high risks and need immediate action.
12. Click **Display Logs**. An **Event Log** table displays at the lower section of the screen.
13. To view details for a particular event, click a link under **Date**. A new screen opens, with the details for the event. For more information, see *Event Details* on page 7-28.
14. (Optional) Mouse over the source IP address or destination IP address results and select from **Monitored Network**, **Registered Domain**, or **Registered Service** to add the IP address to the network configuration lists.
15. (Optional) Click **Print** to print the logs or **Export Logs** to export the file to a `.CSV` file.

Application Filter Logs

Each time Threat Discovery Appliance performs application filtering, Threat Discovery Appliance stores the results in the logs. The log contains the application activities. Threat Discovery Appliance stores these logs in the product's hard drive.

To query application filter logs:

PATH: LOGS > APPLICATION FILTER LOG QUERY

1. Select the protocol type. You can select **Instant Messaging**, **P2P**, or **Streaming Media Traffic**.
2. Select the traffic direction. You can select **Internal attacks**, **External detections**, or both.

3. Select the group name.

TABLE 7-12. Group name options

OPTION	DESCRIPTION
Group name	Select from one of the group names in the list
Specify group name	Type the specific group name the name including deleted group names
Removed group	Select this option if the group name is not available in the list and you cannot remember the exact name, for example, if the group name has been deleted
No group	Select this option for those that do not fall under any of the other categories

4. Select the network zone. You can select from **Trusted**, **Untrusted**, and/or **No network zone**.
5. Specify the date range or click the calendar icon and select the date you want.
6. Select from the IP addresses options. You can select all the IP addresses, a certain IP address, or a range of IP addresses.
7. Specify the MAC address of the client computer.
8. Click **Display Logs**. An **Event Log** table displays at the lower section of the screen.
9. To view details for a particular event, click a link under **Date**. A new screen opens, with the details for the event. For more information, see *Event Details* on page 7-28.
10. (Optional) Click **Print** to print the logs or **Export Logs** to export the file to a `.CSV` file.

System Logs

Threat Discovery Appliance stores system events and component update results in the logs. Threat Discovery Appliance stores these logs in the product's hard drive.

To query system logs:

PATH: LOGS > SYSTEM LOG QUERY

1. Select a log type. Select **System events**, **Update events**, or both.
2. Specify the date range or click the calendar icon to select a specific date.
3. Click **Display Logs**.

Syslog Server

If you have set up Syslog servers to maintain and organize logs coming from different products, configure Threat Discovery Appliance to send logs to the Syslog servers.

To send logs to Syslog servers:

PATH: LOGS > SYSLOG SERVER SETTINGS

1. Select **Enable Syslog Server**.
2. Type the IP address and port number of the Syslog server.
3. Select the syslog facility and severity.
4. Select the logs to send to the Syslog server.
5. Click **Save**.

Event Details

Threat Discovery Appliance logs the details of each Internet threat it identifies. The Event Details screen on the product console may contain any of the following information, depending on the protocol, file and other factors:

Security Risk Details

TABLE 7-13. Security risk details

NAME	DESCRIPTION
Date	Date and time the incident occurred
VLAN ID	Virtual local area network ID
Detection name	Name of the known threat
Detection by	Scan engine that detected the threat
Traffic direction	File/detection direction
Type	Type of Internet threat
Detection Type	Type of detection, such as Potential threat, Known threat, or Outbreak Containment Service
Severity	Degree of potential risk of the threat
Protocol	Protocol used by the threat
Intelligent rule ID	Network Content Correlation Engine rule number triggered by the file
Suspicious behavior	Network Content Correlation Engine rule reason triggered by the session data or network traffic
Mitigation	Status of mitigation (Mitigated or Un-Mitigated)
Outbreak Containment Services	Status of block action (Blocked or Un-Blocked)
Host name	Host or product name
Source IP address	IP address and host name of the source of the threat
Source port	Port number of the source of the threat

TABLE 7-13. Security risk details (Continued)

NAME	DESCRIPTION
Source MAC address	MAC address and vendor name of the source of the threat
Source group	Group name of the source of the threat
Source network zone	Network zone of the source of the threat
Source Active Directory Domain\Account	Active Directory domain name and account used to log on to the source of the threat and the corresponding timestamp
Destination IP address	IP address and host name of the threat destination
Destination port	Port number of the threat destination
Destination MAC address	MAC address of the threat destination
Destination group	Group name of the threat destination
Destination network zone	Network zone of the threat destination
Destination Active Directory Domain\Account	Active Directory domain name and account used to log on to the destination of the threat

<Protocol> Details

TABLE 7-14. Event details for traffic through various protocols

NAME	DESCRIPTION
User name	Name of the logged on user
Sender	Email address that sent the suspicious file
Recipient	Email address of the suspicious file recipient
Subject	Subject of the suspicious email
User agent	Client application used with a particular network protocol
Target share	Shared folder where the malicious file is dropped
Channel name	Name of the IRC channel

File Details

TABLE 7-15. File details

NAME	DESCRIPTION
File name	Name of the file tagged as a potential/known risk
File size	Size of the file tagged as a potential/known risk
File extension	Extension of the file tagged as potential/known risk
File name in archive	Name of the file in the archive tagged as potential/known risk

Additional Details

TABLE 7-16. Additional event details

NAME	DESCRIPTION
Authentication	Whether the protocol requires authentication
URL	Link included in the email or the instant message content
BOT command	Command used in IRC for BOTs
BOT URL	URL used in IRC for BOTs
Constraint Type	Reasons Threat Discovery Appliance stops scanning files in the network

Chapter 8

Maintenance

This chapter explains how to perform maintenance tasks for Threat Discovery Appliance.

The topics discussed in this chapter are:

Web Console Timeout

Configure how long Threat Discovery Appliance waits before logging out an inactive web console user session.

To configure web console timeout settings:

PATH: ADMINISTRATION > WEB CONSOLE TIMEOUT

1. Type the number of minutes. The value must be between 1 and 30.
2. Click **Save**.

Log Maintenance

Threat Discovery Appliance maintains the logs in the product's hard disk and displays them on the Log Maintenance screen on the product console. Manually delete logs on a regular basis to keep the size of logs from occupying too much space on the hard disk. Deletion of logs depends on your environment and the quantity of logs that you want to retain.

Threat Discovery Appliance automatically deletes logs if 1,000,000 logs have been accumulated. One percent of the logs are automatically deleted, beginning with the oldest logs.

Note: Threat Discovery Appliance can send logs to a Syslog server or Trend Micro Control Manager. For details, see *Syslog Server* on page 7-28 and *Trend Micro Control Manager* on page 6-29.

You can also view the status of the product database and repair corrupted database files from the Log Maintenance screen.

To configure log maintenance settings:

PATH: LOGS > LOG MAINTENANCE

1. Select the logs you want to delete. For example, you can select all logs under **Known Threats/Risk Logs** and **System Logs**, or you can **Select all** logs.
2. Select an option under action. You can select to **Delete all logs selected above** or **Delete logs selected above older than** the specified number of days you chose.
3. Click **Delete Now**.

To perform maintenance tasks for the product database:

PATH: LOGS > LOG MAINTENANCE

1. Click **Check Database**.
2. If one or more database files are corrupted, click **Repair**. The product begins to repair the corrupted files and informs you of the status.

Configuration Backup and Restore

Configuration settings include both the Threat Discovery Appliance and network configuration settings. You can back up the settings by exporting them to an encrypted file. You can then import the file to restore settings in case of a problem.

You can also reset Threat Discovery Appliance by restoring the default settings that shipped with the product.

Take note of the following:

- Most or all settings on the following screens are not backed up:
  - Threat Management Services Portal
  - Mitigation Devices
  - Mitigation Exclusion List
  - Security Compliance
  - Trend Micro Control Manager
  - Network Interface Settings
  - Licenses and Activation Codes
  - Smart Protection Settings in the Web Reputation screen

- The encrypted file cannot be modified.
- Importing an encrypted file overwrites all the current settings on Threat Discovery Appliance.
- The encrypted file can also be used to replicate settings on another Threat Discovery Appliance.

To back up settings to an encrypted file:

PATH: ADMINISTRATION > BACKUP/RESTORE

1. Click **Backup** under **Backup Current Configuration**. A File Download screen displays.
2. Click **Save**, browse to the target location of the file, and then click **Save**.

To import an encrypted file:

PATH: ADMINISTRATION > BACKUP/RESTORE

1. Before importing a file, back up the current configurations by performing the steps under *To back up settings to an encrypted file:* on page 8-4.
2. Click **Browse** under **Restore Configuration (from backup)**. The Choose File screen appears.
3. Select the encrypted file to import and click **Restore Configuration**. A confirmation message appears.
4. Click **OK**. Threat Discovery Appliance restarts after importing the configuration file.

To restore the default settings that shipped with the product:

PATH: ADMINISTRATION > BACKUP/RESTORE

1. Before restoring settings, back up the current configurations by performing the steps under *To back up settings to an encrypted file:* on page 8-4.
1. Click **Reset to Default Settings**. A confirmation message appears.
2. Click **OK**. Threat Discovery Appliance restarts.

Firmware Update

Trend Micro may release a new firmware so you can upgrade the product to a new version or enhance its performance. You can choose to migrate the current settings on the product after the update is complete so that you do not need to re-configure settings.

Before updating the firmware:

1. Back up configuration settings. For details, see *Configuration Backup and Restore* on page 8-3.
2. If you have registered Threat Discovery Appliance to Control Manager, record the Control Manager registration details. You need to re-register to Control Manager after the firmware update is complete.
3. Download the Threat Discovery Appliance firmware image from the Trend Micro website or obtain the image from your Trend Micro reseller or support provider.
4. Save the image to any folder on a computer.

To update the firmware:

PATH: ADMINISTRATION > FIRMWARE UPDATE

1. Click **Browse** and then locate the folder to which you saved the firmware image (the image file has an .R extension).
2. Click **Upload Firmware**. The Migration configuration option appears. Enable this option to retain the current product settings after the update, or disable it to revert to the product's default settings after the update.

Note: Performing the next step will restart Threat Discovery Appliance. Ensure that you have finished all your product console tasks before performing this next step.

---

3. Click **Continue**. Threat Discovery Appliance restarts after the update. The Log on screen appears after the product restarts.

Note: When Threat Discovery Appliance starts, it checks the integrity of its configuration files. The product console password may reset if the configuration file containing password information is corrupted. If you are unable to log on to the console using your preferred password, log on using the default password **admin**.

After updating the firmware:

1. If Threat Discovery Appliance is registered to Control Manager, register the product again. For details, see *Trend Micro Control Manager* on page 6-29.

System Updates

After an official product release, Trend Micro may release system updates to address issues, enhance product performance, or add new features.

System Update Types

Trend Micro may release the following types of system updates:

TABLE 8-1. System updates

SYSTEM UPDATE	DESCRIPTION
Hot fix	A hot fix is a workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore are not released to all customers. For non-Windows hot fixes, applying a hot fix typically requires stopping program daemons, copying the hot fix file to overwrite its counterpart in your installation, and restarting the daemons.
Security patch	A security patch focuses on security issues suitable for deployment to all customers. Non-Windows patches commonly have a setup script.

TABLE 8-1. System updates (Continued)

SYSTEM UPDATE	DESCRIPTION
Patch	A patch is a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Non-Windows patches commonly have a setup script.
Service pack	A service pack is a consolidation of hot fixes, patches, and feature enhancements significant enough to be a product upgrade. Non-Windows service packs include a Setup program and Setup script.

Your vendor or support provider may contact you when these items become available. Check the Trend Micro website for information on new hot fix, patch, and service pack releases:

http://www.trendmicro.com/download

System Update Rollback

Threat Discovery Appliance has a rollback function that allows you to undo a system update and revert the product to its pre-update state. Use this function if you encounter problems with the product after a particular system update is applied.

Only the latest system update can be rolled back. After a rollback, none of the other existing system updates can be rolled back. The rollback function will only become available again when a new system update is applied.

Before performing a system update:

1. Save the system update file to any folder on a computer.

   WARNING! Save the system update file using its original name to avoid problems applying it.

2. All releases include a readme file that contains installation, deployment, and configuration information. Read the readme file carefully before applying the system update.

   Tip: The readme file should indicate if a system update requires Threat Discovery Appliance to restart. If a restart is required, ensure that all tasks on the console have been completed before applying the update.

3. On the computer where you saved the file, access and then log on to the web console.

To apply system updates:

PATH: ADMINISTRATION > SYSTEM UPDATE

1. Click **Browse** and then locate the system update file.
2. Click **Upload**.

   WARNING! To avoid problems uploading the file, do not close the browser or navigate to other screens.

3. If the upload was successful, check the **Uploaded System Update Details** section.

   This section indicates the build number for the system update that you just uploaded and if a restart is required.

   If a restart is required, finish all tasks on the console before proceeding. You will be redirected to the web console's logon screen after the update is applied.

4. Click **Continue** to apply the system update.

WARNING! **To avoid problems applying the system update, do not close the browser or navigate to other screens.**

Note: If there are problems applying the system update, details will be available in the System Update screen, or in the Summary screen if a restart is required.

5. Skip this step if a restart is not required.

   If a restart is required:

   a. Log on to the web console.

   b. Check the Summary screen for any problems encountered while applying the system update.

   c. Navigate back to the System Update screen.

6. Verify that the system update displays in the **System Update Details** section as the latest update.

   The system update also appears as the first entry under the **System update history** table. This table lists all the system updates that you have applied or rolled back. A link to the readme file is conveniently provided in the last column of the table.

7. If you encounter a problem with the product after applying the update:

   a. Check the readme for the system update for any rollback instructions or notes. For example, if a rollback requires a restart, ensure that all tasks on the console have been completed before rollback because the rollback process automatically restarts Threat Discovery Appliance.

   b. Click **Roll Back**.

   c. Check the rollback result in the first row of the **System update history** table. A rollback does not remove the readme file, so you can refer to it at any time for details about the system update.

Restart or Shutdown

Shut down or restart Threat Discovery Appliance or its associated services from the **System Maintenance** screen on the product console.

When Threat Discovery Appliance starts, it checks the integrity of its configuration files. The product console password may reset if the configuration file containing password information is corrupted. If you are unable to log on to the console using your preferred password, log on using the default password **admin**.

To shut down Threat Discovery Appliance:

PATH: ADMINISTRATION > SYSTEM MAINTENANCE

1. Select **Shut down** under System Maintenance.
2. (Optional) Specify a reason for shutting down the product.
3. Click **Ok**.

To restart Threat Discovery Appliance or its services:

PATH: ADMINISTRATION > SYSTEM MAINTENANCE

1. Click **Restart**.
   a. To restart Threat Discovery Appliance, click **System**.
   b. To restart services, click **Service**.
2. (Optional) Specify a reason for restarting the services beside **Comment**.
3. Click **Ok**.

Appliance Rescue

Rescuing the software appliance means reinstalling the product's application and reverting to saved or default settings.

As an alternative, you can use the web console to rescue the software appliance (see *Configuration Backup and Restore* on page 8-3) or update the firmware (see *Firmware Update* on page 8-5).

You might need to rescue the software appliance if the application files become corrupted. Rescuing the software appliance reinstalls the Threat Discovery Appliance application that instructs Threat Discovery Appliance to monitor traffic and create logs.

Rescuing the software appliance is not the same as applying a system update:

- **Rescuing:** Replaces application files and keeps or restores the default settings.
- **Applying a system update:** Updates the existing application files to enhance features.

WARNING! **Before rescuing the software appliance, create a backup of your settings. For details, see *Configuration Backup and Restore* on page 8-3).**

To enter rescue mode:

1. Log on to the Preconfiguration Console through a serial connection to the management port. For details, see *The Preconfiguration Console* on page 4-2).
2. Type **4** and press [Enter]. The System Tasks screen appears.

3. Type **5** and press [Enter]. The Reset Device screen appears.

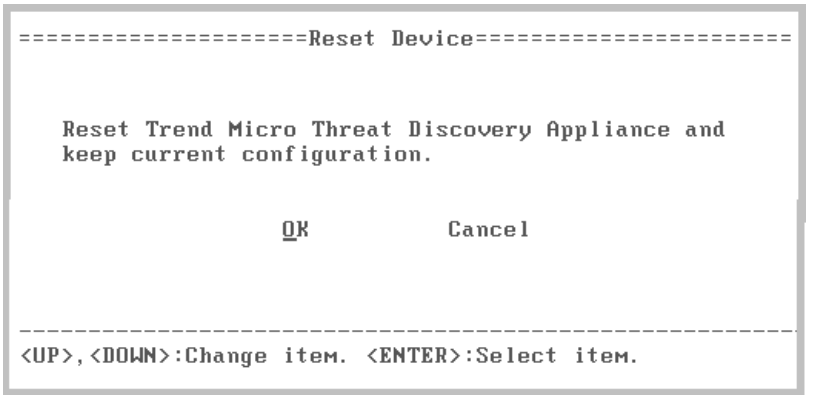


FIGURE 8-1. The Reset Device screen

4. Select **OK**. The software appliance restarts.

5. When the *Press the ESC button* message appears in the boot screen, press [Esc] immediately. The boot menu appears.

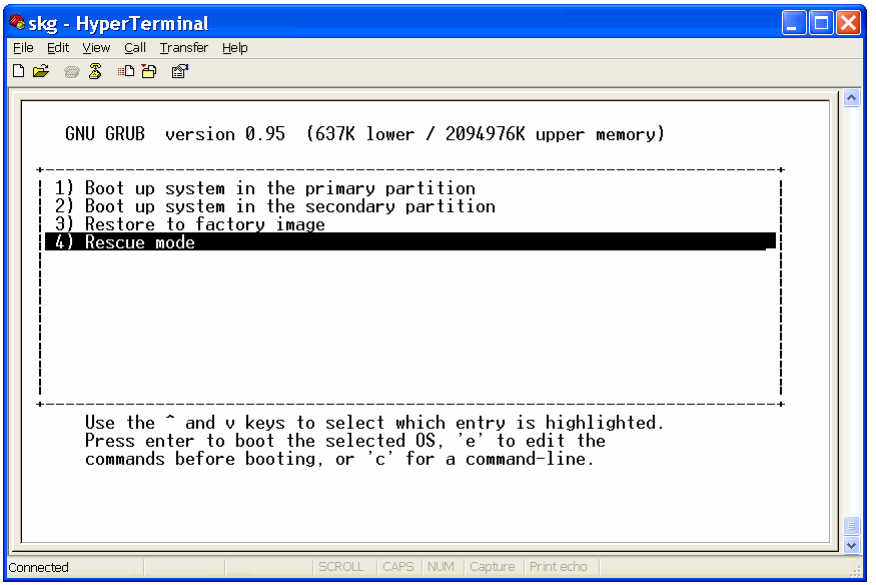


FIGURE 8-2. The Boot menu

6. Type **4** and press [Enter]. The Threat Discovery Appliance rescue mode screen appears.

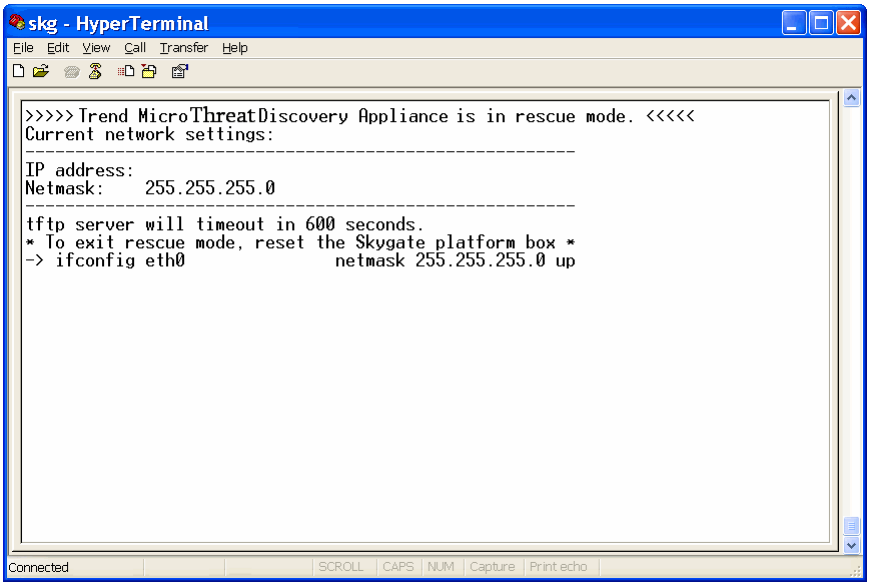


FIGURE 8-3. The Threat Discovery Appliance rescue mode screen

7. Locate the Threat Discovery Appliance Rescue Tool (`TDARescue.exe`). Double-click the tool.

WARNING! **Ensure you are in Rescue mode before using the Rescue Tool.**

8. Browse to the latest image file.
9. Click **Update**. The Threat Discovery Appliance Rescue Tool uploads the new image.

Note: During the update, do not turn off or reset the appliance.

10. After the file uploads successfully, click **Finish**.

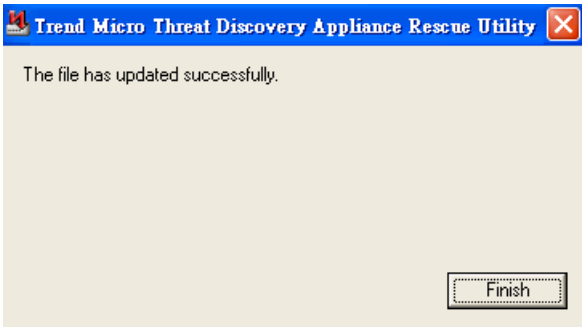


FIGURE 8-4. File upload successful

11. In HyperTerminal, type **Y** to migrate the previous configuration files. Press [Enter] to continue. Threat Discovery Appliance starts migrating the configuration files.

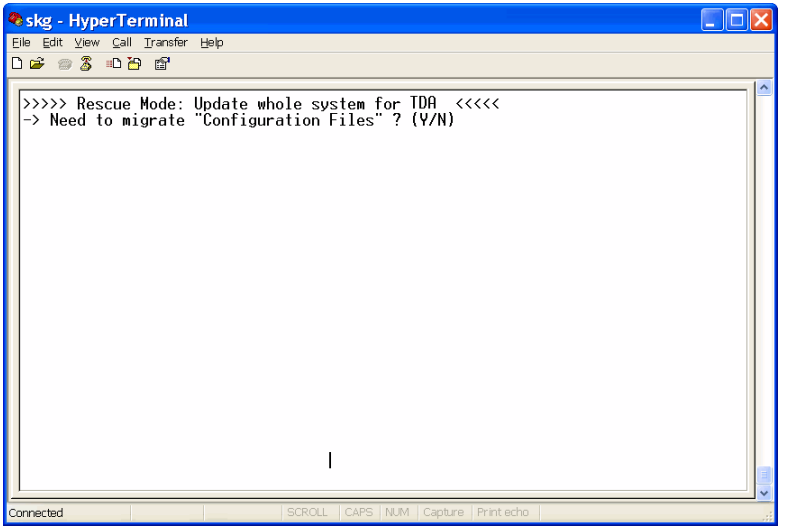


FIGURE 8-5. The configuration file migration screen

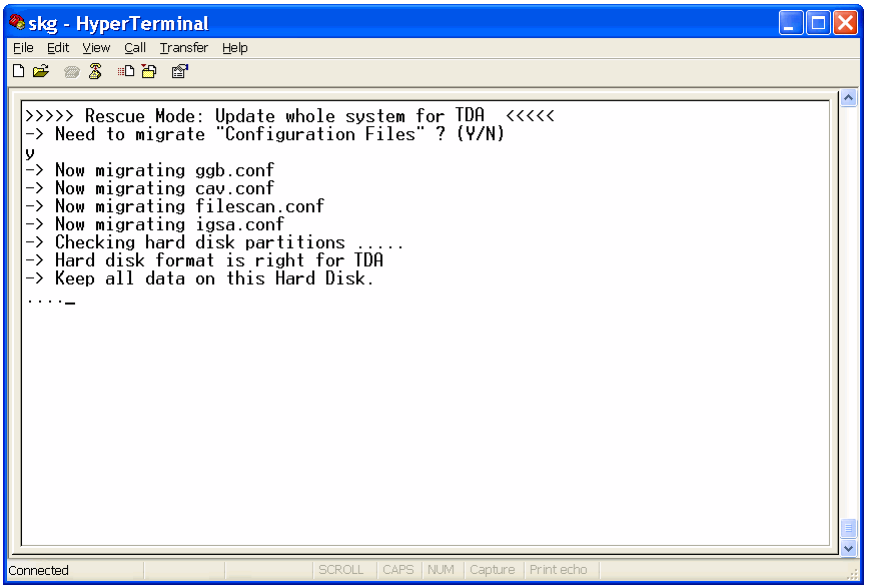


FIGURE 8-6. Configuration migration screen

12. After migration, open the Preconfiguration Console and configure the Threat Discovery Appliance network settings (see *Preconfiguration Menu: Device Settings* on page 4-7).

Chapter 9

Getting Help

This chapter answers questions you might have about Threat Discovery Appliance and describes how to troubleshoot problems that may arise.

The topics discussed in this chapter are:

Frequently Asked Questions (FAQs)

The following is a list of frequently asked questions and answers.

Installation

Will the Threat Discovery Appliance installation disrupt network traffic?

No. Threat Discovery Appliance installation should not disrupt the network traffic since the product connects to the mirror port of the switch and not directly to the network.

Activation

Do I need to activate Threat Discovery Appliance after installation?

Yes. Use a valid Activation Code to enable the Threat Discovery Appliance features. Additionally, you can register to TMSP and get daily and weekly threat analysis reports.

Configuration

How many seconds of inactivity does the Preconfiguration Console accept before logging off?

After five minutes of inactivity, Threat Discovery Appliance logs out of the inactive session.

Can I register Threat Discovery Appliance to more than one Control Manager server?

No, you cannot register Threat Discovery Appliance to more than one Control Manager server. To register Threat Discovery Appliance to a Control Manager server, refer to *Trend Micro Control Manager* on page 6-29.

Will changing the Threat Discovery Appliance IP address prevent it from communicating with the Control Manager server?

Yes, changing the Threat Discovery Appliance IP address through the Preconfiguration Console or product console will cause temporary disconnection (30 seconds). During the time the MCP agent is disconnected from Control Manager, the MCP agent logs off from Control Manager and then logs on and provides Control Manager with the updated information.

I typed the wrong password three times when logging on to the Preconfiguration Console. Then, I could no longer log on to the Preconfiguration Console. What should I do?

If you typed the wrong password three consecutive times, the product will lock for 30 seconds before you can try to log on again. Wait for 30 seconds and try to log on again if this happens.

Is there anything that the administrator needs to configure in the firewall settings?

If you use Threat Discovery Appliance only for monitoring the network, you do not need to configure the firewall settings. However, if Threat Discovery Appliance connects to the Internet for updates or to TMSP, you need to configure the firewall to allow Ports 80, 22 or 443 traffic from Threat Discovery Appliance.

I am unable to register to TMSP, what can I do?

Ensure that:

- The TMSP logon details are correct.
- Ensure that you have configured your firewall settings to allow port 22 or 443 traffic.
- Ensure that you are using the correct proxy settings.

If the problem persists, consult your support provider.

Product Updates

By default, where does Threat Discovery Appliance download updated components from?

Threat Discovery Appliance receives updated components from the Trend Micro ActiveUpdate server by default. If you want to receive updates from other sources, configure an update source for both scheduled and manual updates.

How often should I update Threat Discovery Appliance?

Trend Micro typically releases virus pattern files on a daily basis and recommends updating both the server and clients daily. You can preserve the default schedule setting in the Scheduled Update screen to update the product every 2 hours.

Does Threat Discovery Appliance restart during an update?

Yes, Threat Discovery Appliance needs to restart if there is an update for the Network Content Inspection Engine and Threat Discovery Appliance firmware. For scheduled updates, Threat Discovery Appliance sends an email to the user to click the **Restart** button in the product console. For manual updates, the **Restart** button appears in the Manual Update screen until you restart the product.

Why does Threat Discovery Appliance still use the old components after updating the software and restarting the product?

Updating Threat Discovery Appliance components follows the product constraints. This means that when updating components, the product updates the software first. Restart the product and update the Network Content Inspection Engine. Restart the product again before updating the other components.

Logs

Why does the Log Query screen display no result or takes a long time before the results appear?

When Threat Discovery Appliance queries the database and there is a heavy volume of traffic and logs, there might be some delay in displaying the information. Please wait for the information to show. Do not click anything or Threat Discovery Appliance might start to query the logs once again.

Documentation

What documentation is available with this version of Threat Discovery Appliance?

This version of Threat Discovery Appliance includes the following documentation:

- Administrator's Guide
- Readme file
- Help

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

Creating a New Virtual Machine

This appendix describes how to create a new virtual machine that will host Threat Discovery Appliance.

Creating a New Virtual Machine

The actual installation of VMware ESX is not covered in this document. Please refer to the VMware product documentation to install this product.

The steps outlined below detail the process for creating a new virtual machine in VMware ESX to install Threat Discovery Appliance. Please use the following steps as a guideline for creating the virtual machine for your environment. The number of CPUs, NICs, memory, and hard disk space selected should reflect the Threat Discovery Appliance requirements listed in *System Requirements* on page 3-2.

Note: The screens in this procedure may appear in a different order and the options available in each screen may vary depending on the VMware ESX version.

To create the virtual machine:

1. From the VMware ESX menu bar, select **File > New > Virtual Machine**.

2. When the Configuration screen appears, click **Custom** and then click **Next**.

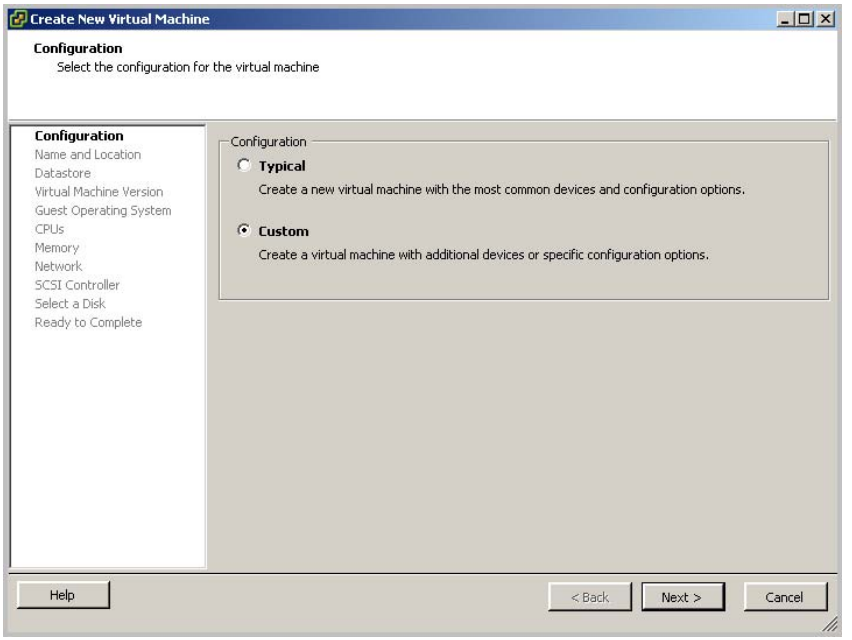


FIGURE A-1. Configuration screen

3. When the Name and Location screen appears, type a name for the virtual machine and then click **Next**.

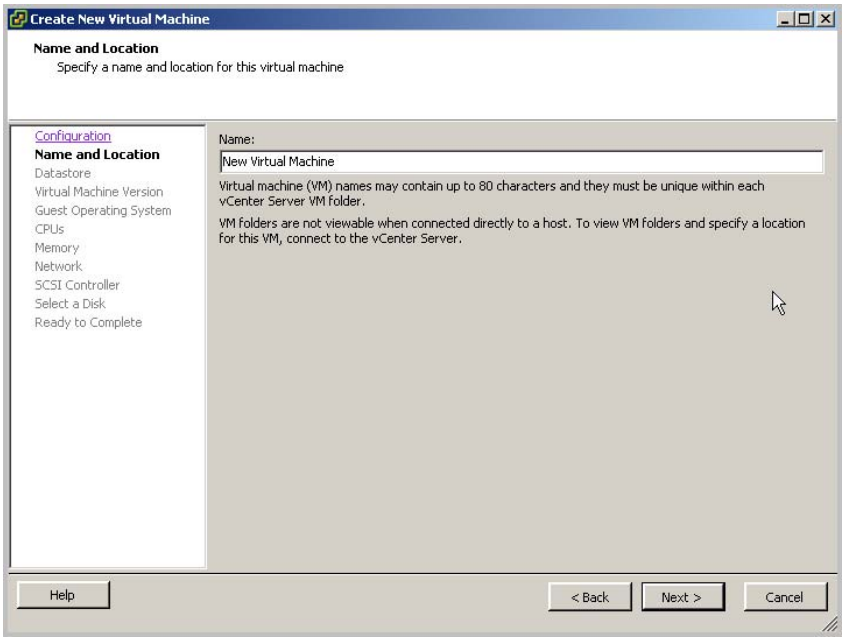


FIGURE A-2. Name and Location screen

4. When the Datastore screen appears, select the datastore where the virtual machine will reside and then click **Next**.

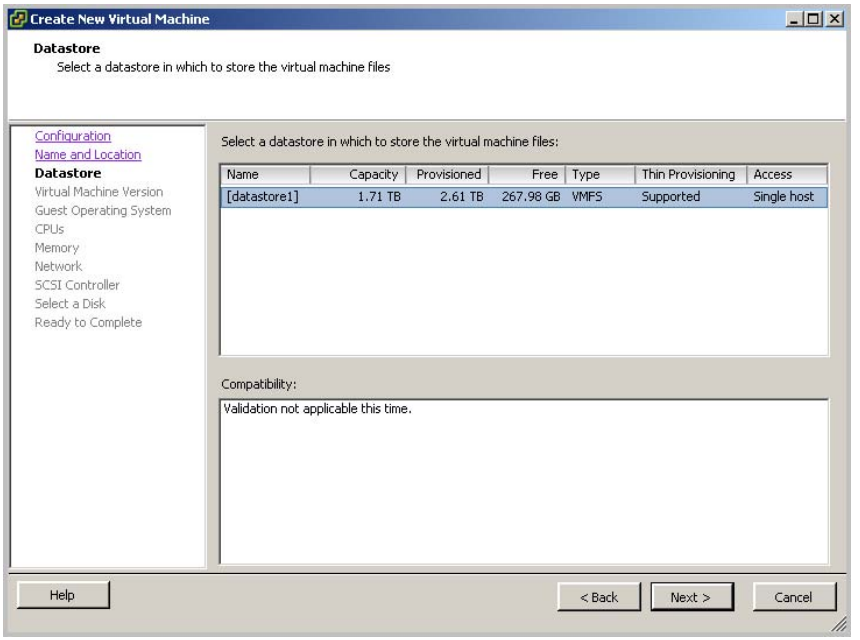


FIGURE A-3. Datastore screen

5. When the Virtual Machine Version screen appears, select the virtual machine version to use and then click **Next**.

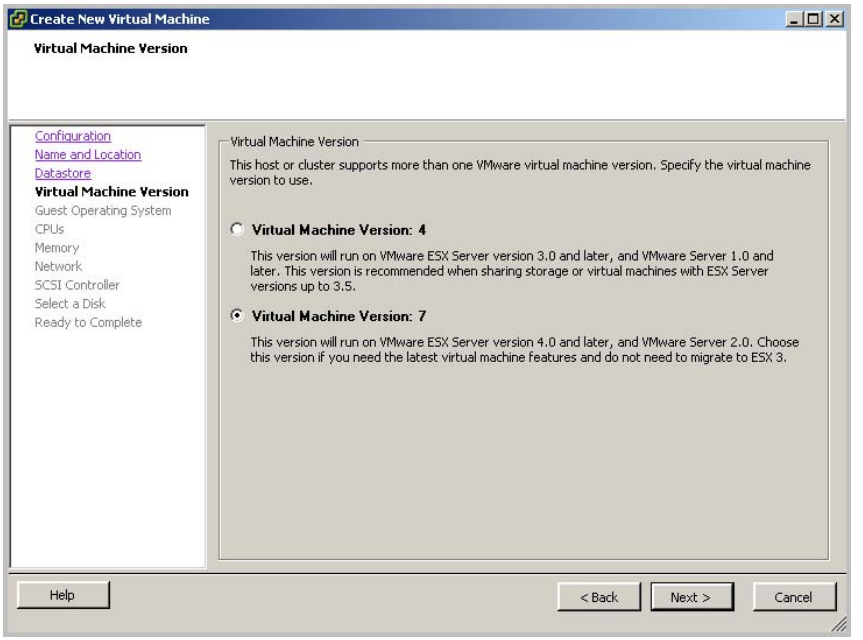


FIGURE A-4. Virtual Machine Version screen

6. When the Guest Operating System screen appears, select **Linux > Other Linux (64-bit)** and then click **Next**.

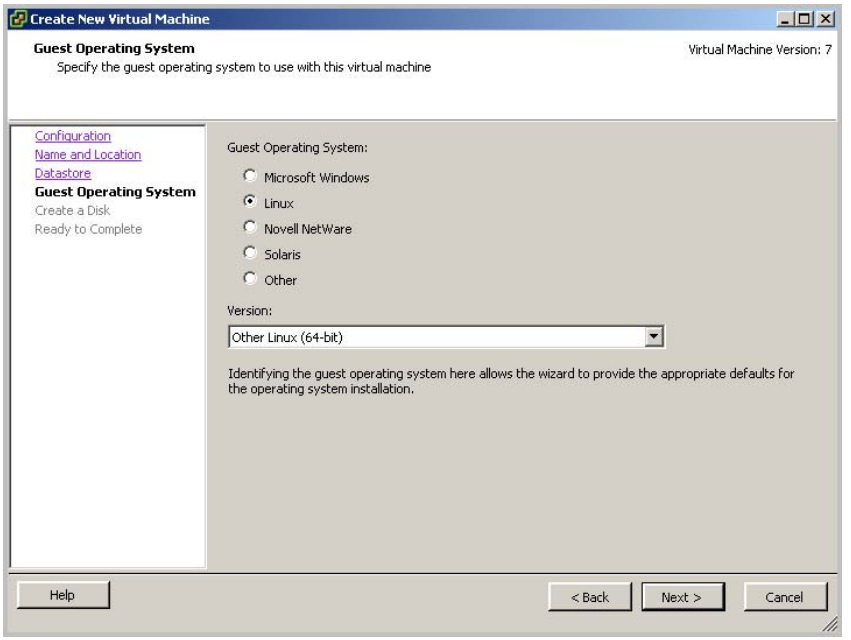


FIGURE A-5. Guest Operating System screen

7. When the CPUs screen appears, select the number of processors for the virtual machine and then click **Next**.

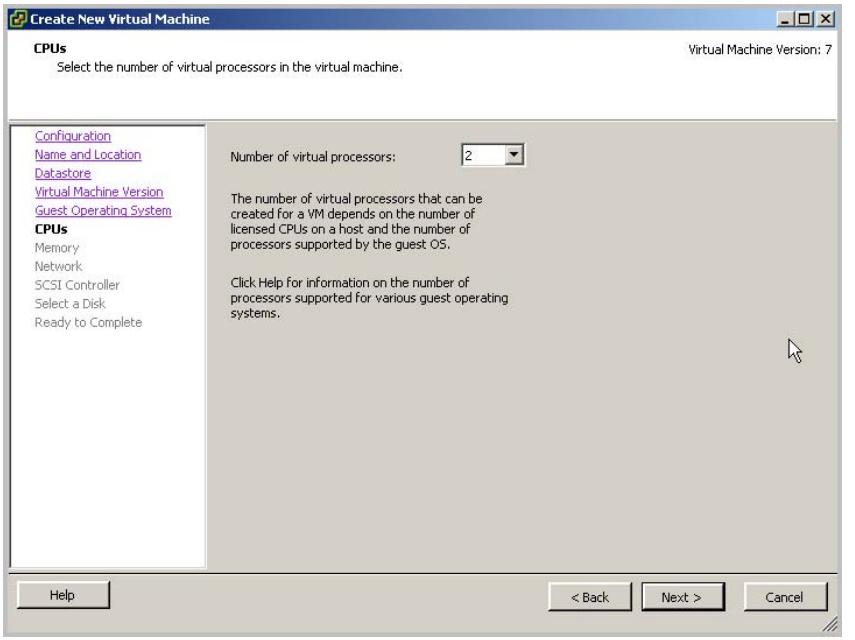


FIGURE A-6. CPUs screen

Tip: Threat Discovery Appliance takes advantage of the Virtual SMP, so select the maximum number of virtual processors available.

8. When the Memory screen appears, allocate at least 2GB (2048MB) of memory for Threat Discovery Appliance and then click **Next**.

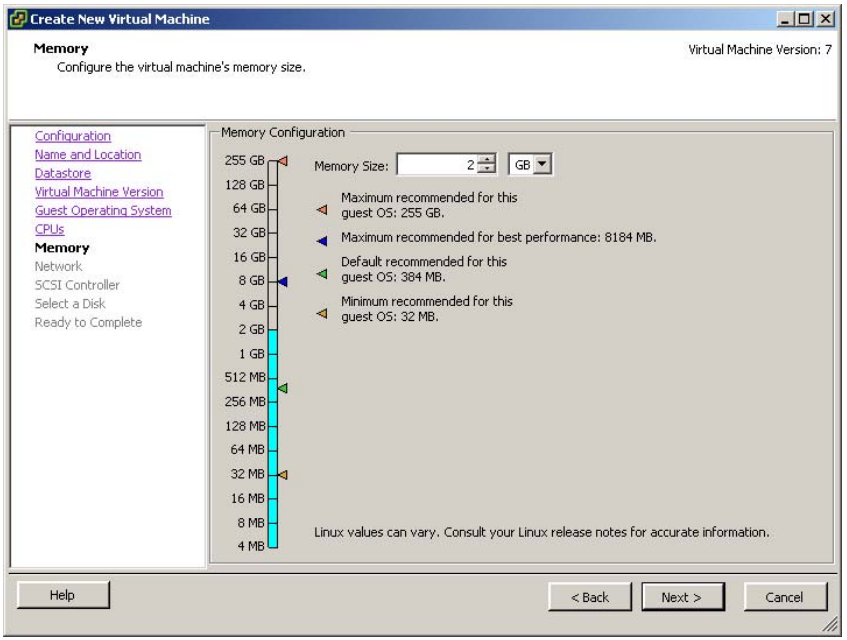


FIGURE A-7. Memory screen

9. When the Network screen appears, configure at least two NICs for Threat Discovery Appliance and then click **Next**.

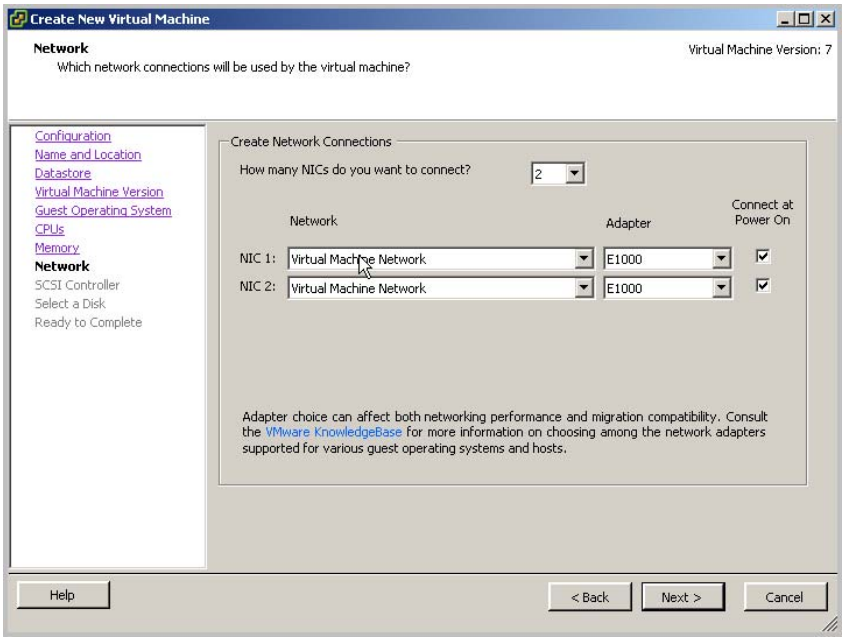


FIGURE A-8. Network screen

10. When the SCSI Controller screen appears, select the I/O adapter type that is appropriate for your virtual disk and then click **Next**.

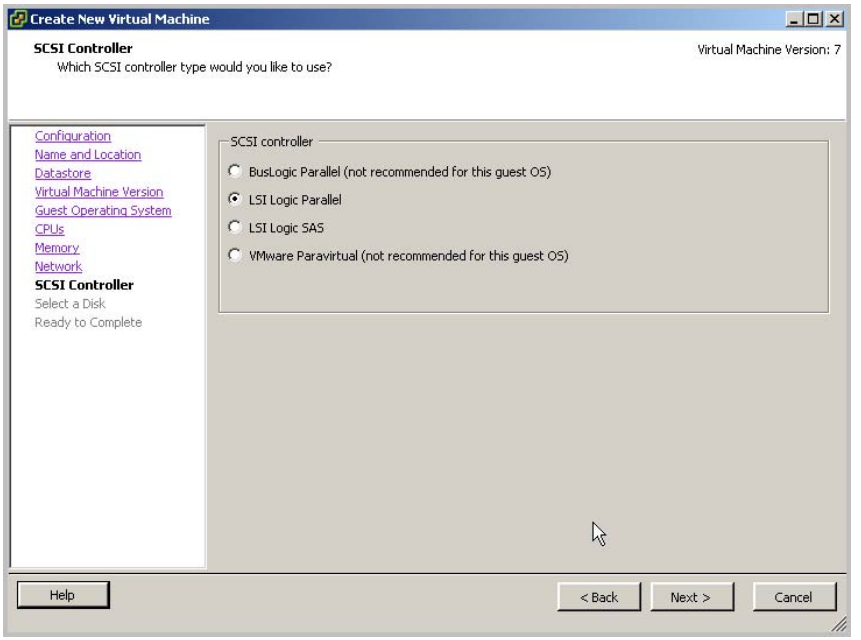


FIGURE A-9. SCSI Controller screen

11. When the Select a Disk screen appears, select the type of disk to use (**Create a new virtual disk** in this procedure) and then click **Next**.

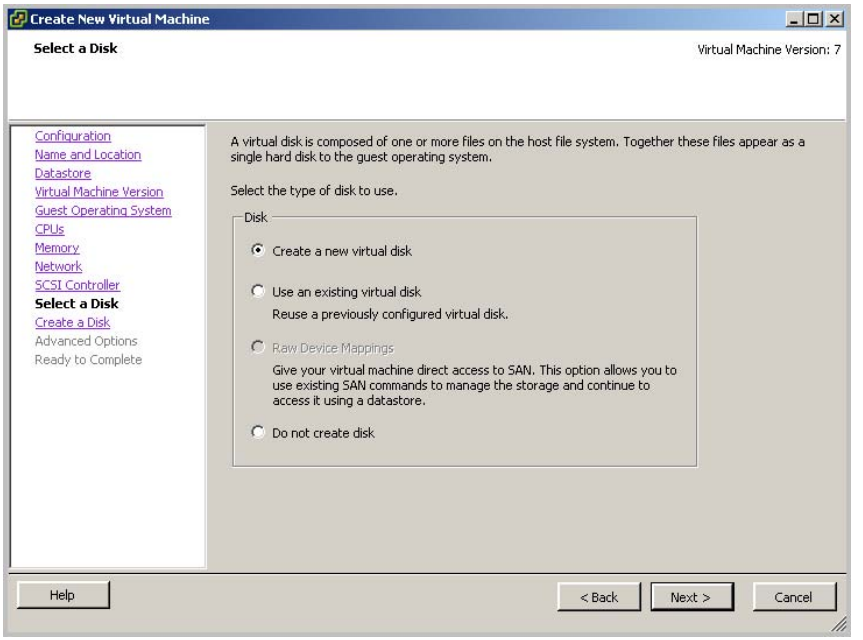


FIGURE A-10. Select a Disk screen

12. When the Create a Disk screen appears, allocate at least 6.5GB hard disk space for Threat Discovery Appliance and then click **Next**.

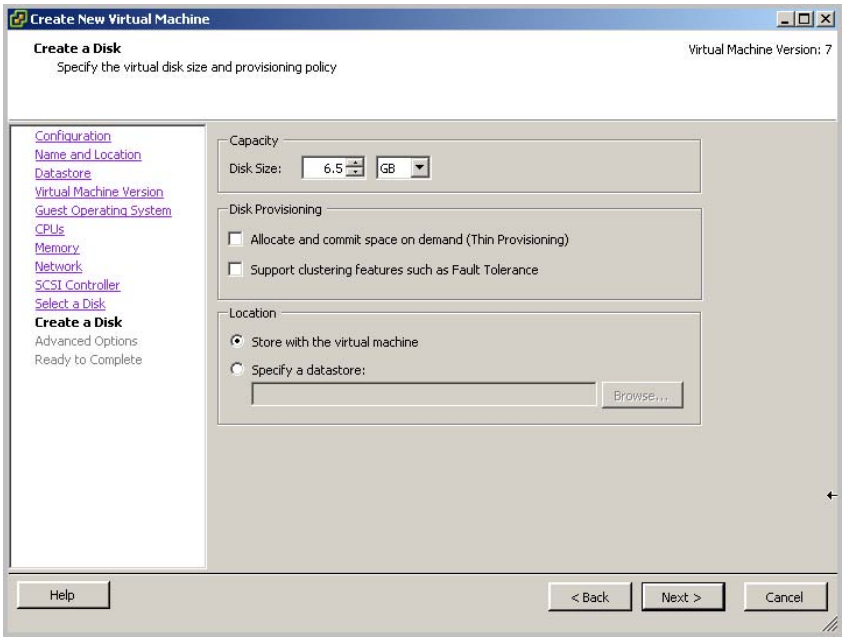


FIGURE A-11. Create a Disk screen

13. When the Advanced Options screen appears, leave the default selections and then click **Next**.

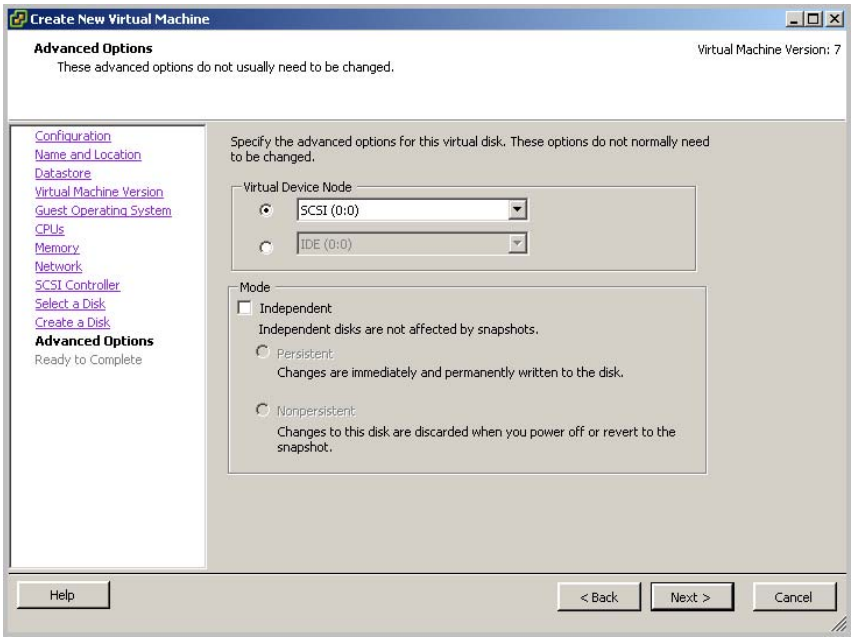


FIGURE A-12. Advanced Options screen

14. When the Ready to Complete screen appears, review the settings and click **Finish**.

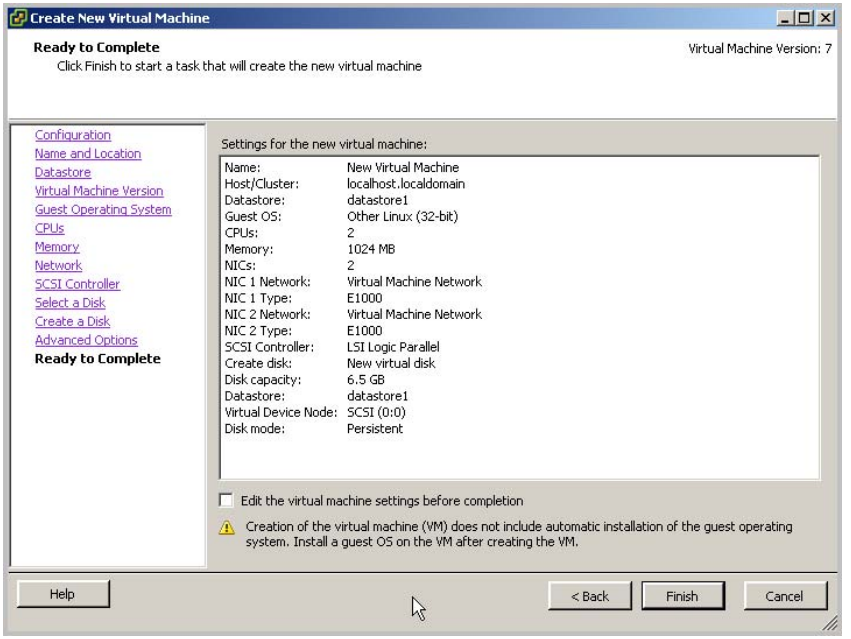


FIGURE A-13. Ready to Complete screen

The new virtual machine is now ready.

Appendix B

Glossary

This glossary describes terms used in Threat Discovery Appliance documentation.

TABLE B-1. Glossary of Terms

TERM	DEFINITION
Active	This refers to the device currently in use.
ActiveUpdate	ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update website, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, program, and other Trend Micro component files through the Internet or the Trend Micro Total Solution CD.
ActiveX	A type of open software architecture that implements object linking and embedding, enabling some of the standard interfaces, such as downloading of web pages.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
ActiveX malicious code	An ActiveX control is a component object embedded in a web page which runs automatically when viewing the page. ActiveX controls allow web developers to create interactive, dynamic web pages with broad functionality such as HouseCall, Trend Micro's free online scanner. Hackers, virus writers, and others who want to cause mischief or worse may use ActiveX malicious code as a vehicle to attack the system. Change the browser's security settings to "high" so that these ActiveX controls do not execute.
Address	Refers to a networking address (*see* IP address) or an email address, which is the string of characters that specify the source or destination of an email message.
Administrator	Refers to "system administrator"—the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing back ups, and managing network security.
Administrator account	A user name and password that has administrator-level privileges.
Administrator email address	The address used by the administrator of your Trend Micro product to manage notifications and alerts.
Adware	Advertising-supported software in which advertising banners display while the program is running. *See also* Spyware.
Alert	A message intended to inform a system's users or administrators about a change in the operating conditions of that system or about some kind of error condition.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Antivirus	Computer programs designed to detect and clean computer viruses.
Archive	A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.
Attachment	A file attached to (sent with) an email message.
Authentication	The verification of the identity of a person or a process. Authentication ensures that the system delivers the digital data transmissions to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a user name and password to gain access to a particular account. Other authentication protocols are secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or public-key systems using digital signatures. *Also see* public-key encryption *and* digital signature.
Boot sector	A sector is a designated portion of a disk (the physical device from which the computer reads and writes the data on). The boot sector contains the data used by your computer to load and initialize the computer's operating system.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Boot sector virus	A boot sector virus is a virus targeted at the boot sector (the operating system) of a computer. Computer systems are most vulnerable to attack by boot sector viruses when you boot the system with an infected disk from the floppy drive - the boot attempt does not have to be successful for the virus to infect the hard drive. Also, there are a few viruses that can infect the boot sector from executable programs. These are multi-partite viruses and they are relatively rare. Once the system is infected, the boot sector virus will attempt to infect every disk accessed by that computer. In general, most antivirus software can successfully remove boot sector viruses.
Bridge	A device that forwards traffic between network segments based on data link layer information. These segments have a common network layer address.
Browser	A program that allows a person to read hypertext, such as Internet Explorer. The browser gives some means of viewing the contents of nodes (or "pages") and of navigating from one node to another. A browser acts as a client to a remote web server.
Cache	A small fast memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network.
COM file infector	An executable program with a .com file extension. *Also see* DOS virus.
Compressed file	A single file containing one or more separate files plus information for extraction by a suitable program, such as WinZip.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Configuration	Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
Cookie	A mechanism for storing information about an Internet user, such as name, preferences, and interests, which is stored in your web browser for later use. The next time you access a website for which your browser has a cookie, your browser sends the cookie to the web server, which the web server can then use to present you with customized web pages. For example, you might enter a website that welcomes you by name.
Daemon	A program not explicitly invoked, but lays dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.
Default	A value that pre-populates a field in the management console interface. A default value that represents a logical choice and provided for convenience. Use default values as-is, or change them.
Denial of Service (DoS) attack	Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.
Dialer	A type of Trojan that, when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge.
Digital signature	Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption. *Also see* public-key encryption *and* authentication.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Directory	A node, which is part of the structure on a hierarchical computer file system. A directory typically contains other nodes, folders, or files. For example, *C:\Windows* is the Windows directory in the C drive.
Directory path	The subsequent layers within a directory where a file can be found, for example, the directory path for the ISVW for SMB Quarantine directory is: *C:\Programs\Trend Micro\ISVW\Quarantine*
Disclaimer	A statement appended to the beginning or end of an email message that states certain terms of legality and confidentiality regarding the message.
DNS	Domain Name System—A general-purpose data query service chiefly used in the Internet for translating host names into IP addresses.
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data in a computer in the current zone. Client software in the remote server queries the resolver, which answers the request from its database files.
(Administrative) domain	A group of computers sharing a common database and security policy.
Domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host in the Internet. This process, called "name resolution", uses the Domain Name System (DNS).

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
DOS virus	Also referred to as “COM” and “EXE file infectors.” DOS viruses infect DOS executable programs- files that have the extensions *.COM or *.EXE. Unless they have overwritten or inadvertently destroyed part of the original program's code, most DOS viruses try to replicate and spread by infecting other host programs.
Download (verb)	To transfer data or code from one computer to another. Downloading often refers to transfer from a larger "host" system (especially a server or mainframe) to a smaller "client" system.
Dropper	Droppers are programs that serve as delivery mechanisms to carry and drop viruses, Trojans, or worms into a system.
Dynamic Host Configuration Protocol (DHCP)	A protocol for assigning dynamic IP addresses to devices in a network. With dynamic addressing, a device can have a different IP address everytime it connects to the network. In some systems, the device’s IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Encryption	Encryption is the process of changing data into a form that only the intended receiver can read. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender, and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.
Ethernet	A local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. A variety of cable schemes can run over the Ethernet, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network. The most common form of Ethernet is the 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable.
Executable file	A binary file containing a program in computer language which is ready to be executed (run).
EXE file infector	An executable program with an .exe file extension. *Also see* DOS virus.
False positive	An email message that was "caught" by the spam filter and identified as spam, but is actually not spam.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
FAQ	Frequently Asked Questions—A list of questions and answers about a specific topic.
File	An element of data, such as an email message or HTTP download.
File-infecting virus	File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. Some of these viruses are very destructive and attempts to format the hard drive at a pre-determined time or perform some other malicious action. In many cases, you can successfully remove a file-infecting virus from the infected file. However, if the virus has overwritten part of the program's code, the original file will be unrecoverable
File type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type used to select an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
File name extension	The portion of a file name (such as .dll or .xml) which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.
Firewall	A gateway computer with special security precautions in it, used to service outside network (especially Internet) connections and dial-in lines.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
FPGA	Field Programmable Gate Array - a programmable integrated circuit.
FTP	A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.
Gateway	An interface between an information source and a web server.
Grayware	A category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.
Hacker	*See* virus writer.
Hard disk (or hard drive)	One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks.
Heuristic rule-based scanning	Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.
HTML virus	A virus targeted at Hyper Text Markup Language (HTML), the authoring language used to create information in a web page. The virus resides in a web page and downloads through a user's browser.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
HTTP	Hypertext Transfer Protocol—The client-server TCP/IP protocol used in the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
HouseCall	A free virus scanning and cleaning product from Trend Micro. HouseCall can detect and clean viruses found in your hard drive, but HouseCall does not provide real-time protection. In other words, HouseCall can help you to discover and clean up an existing problem, but will not prevent future ones, nor will HouseCall protect against worms, or mass-mailing programs. For preventive protection, you need Trend Micro security products.
Image	Refers to the Trend Micro Threat Discovery firmware or program file.
Image file	A file containing data representing a two-dimensional scene, in other words, a picture. These files are real world images taken using a digital camera, or generated by the computer using graphics software.
IntelliScan	IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true file type recognition, and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code disguised by a harmless extension name.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Internet	A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.
IP	Internet Protocol—*See* IP address.
IP address	Internet address for a device in a network, typically expressed using dot notation such as 123.123.123.123.
IP gateway	Also called a router, a gateway is a program or a special-purpose device that transfers IP datagrams from one network to another before reaching the final destination.
IT	Information technology, to include hardware, software, networking, telecommunications, and user support.
Java file	Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet transfers its code to your system and the browser's Java Virtual Machine executes the applet.)
Java malicious code	Virus code written or embedded in Java. *Also see* Java file.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
JavaScript virus	JavaScript is a simple programming language developed by Netscape that allows web developers to add dynamic content to HTML pages displayed in a browser using scripts. A JavaScript virus is a virus that targets scripts in the HTML code. This enables the virus to reside in web pages and download to a user's desktop through the user's browser. *Also see* VBscript virus.
Joke program	An executable program that is annoying or causes users undue alarm. Unlike viruses, joke programs do not self-propagate. However, you should still remove these from your system.
KB	Kilobyte—1024 bytes of memory.
Keylogger	Keyloggers are programs that catch and store all keyboard activity. There are legitimate keylogging programs used by corporations to monitor employees and by parents to monitor their children. However, criminals also use keystroke logs to sort for valuable information such as logon credentials and credit card numbers.
L2 devices	Short for layer 2 devices. These devices refer to the hardware devices connected to the Data Link layer of the OSI model. Switches are examples of L2 devices.
L3 devices	Short for layer 3 devices. These devices refer to the hardware devices connected to the Network layer of the OSI model. Routers are examples of L3 devices.
Liquid Crystal Display (LCD)	A 5x7 dot display LCD on the Threat Discovery Appliance front panel capable of displaying 2x16 character messages.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Link (also called hyperlink)	A reference from some point in one hypertext document to some point in another document or another place in the same document. You can distinguish links because these usually have a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking it with a mouse, the browser displays the target of the link.
Listening port	A port utilized for client connection requests for data exchange.
Logic bomb	Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever it meets specified conditions.
Macro	A command used to automate certain functions within an application.
MacroTrap	A Trend Micro utility that performs a rule-based examination of all macro code saved in association with a document. Macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).
Macro virus	Often encoded as application macros and included in a document. Unlike other virus types, macro viruses are not specific to an operating system and can spread through email attachments, web downloads, file transfers, and cooperative applications.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Malware (malicious software)	Programming or files developed for the purpose of doing harm, such as viruses, worms, and Trojans.
Management console	The user interface for your Trend Micro product.
Mass mailer (also known as a Worm)	A malicious program that has high damage potential, because it causes large amounts of network traffic.
Mbps	Millions of bits per second—a measure of bandwidth in data communications.
MB	Megabyte—1024 kilobytes of data.
Message	An email message, which includes the message subject in the message header and the message body.
Message body	The content of an email message.
Message size	The number of KB or MB occupied by a message and its attachments.
Message subject	The title or topic of an email message, such as “Third Quarter Results” or “Lunch on Friday.”
Microsoft Office file	Files created with Microsoft Office tools such as Excel or Microsoft Word.
Mirror port	A configured port on a switch used to send a copy of all network packets from a switch port to a network monitoring connection on another switch port.
Mixed threat attack	Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.
Multi-partite virus	A virus that has characteristics of both boot sector viruses and file-infecting viruses.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Network Address Translation (NAT)	A standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. This allows Trusted networks with privately assigned IP addresses to have access to the Internet. This also means that you do not have to get a registered IP address for every computer in your network.
NetBIOS (Network Basic Input Output System)	An application program interface (API) that adds functionality such as network capabilities to disk operating system (DOS) basic input/output system (BIOS).
NetScreen Redundancy Protocol (NSRP)	A proprietary protocol that provides configuration and run time object (RTO) redundancy and a device failover mechanism for GateLock units in a high availability (HA) cluster.
Network segment	A section of a network that falls within the bounds of bridges, routers, or switches. Dividing an Ethernet into multiple segments is one of the most common ways of increasing available bandwidth on the LAN. IF segmented correctly, most network traffic remains within a single segment, enjoying the full 10 Mbps bandwidth. Hubs and switches connect each segment to the rest of the LAN.
Network Time Protocol (NTP)	Refers to an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Network virus	A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client computers, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure.
Notification (*Also see* action and target)	A message that is forwarded to one or more of the following: - system administrator - sender of a message - recipient of a message, file download, or file transfer The purpose of the notification is to communicate that an action took place, or been attempted, such as a virus being detected in an attempted HTTP file download.
Offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
Open source	Programming code that is available to the general public for use or modification free of charge and without license restrictions.
Operating system	The software which handles tasks such as the interface to peripheral hardware, scheduling tasks, and allocating storage. In this documentation, the term also refers to the software that presents a window system and graphical user interface.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Open System Interconnection (OSI) model	This model defines a networking framework for implementing protocols in seven layers. Passing control from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.
Outgoing	Email messages or other data *leaving* your network, routed out to the Internet.
Packer	A compression tool for executable files.
Partition	A logical portion of a disk. (*Also see* sector, which is a physical portion of a disk.)
Password cracker	An application program used to recover a lost or forgotten password. An intruder can use these applications to gain unauthorized access to a computer or network resources.
Pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. Passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
Payload	Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.
Polymorphic virus	A virus that is capable of taking different forms.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
POP3	Post Office Protocol, version 3—A messaging protocol that allows a client computer to retrieve electronic mail from a server through a temporary connection, for example, a mobile computer without a permanent network connection.
POP3 server	A server which hosts POP3 email, from which clients in your network will retrieve POP3 messages.
Port	A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels in the same network interface on the same computer. Each application program has a unique port number associated with it.
Port mirroring	Method of monitoring network traffic by copying source port or VLAN specific traffic to a destination port for analysis.
Preconfiguration Console	The console used to preconfigure the device.
Proxy	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
Proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
Public-key encryption	An encryption scheme where each person gets a pair of “keys,” called the public key and the private key. The software publishes the public key while keeping the private key a secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his or her private key. *Also see* authentication *and* digital signature.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Purge	To delete all, as in getting rid of old entries in the logs.
Recipient	The person or entity to whom an email message is addressed.
Relay	To convey by means of passing through various other points.
Remote Port Mirroring	An implementation of port mirroring designed to support source ports, source VLANs, and destination ports across different switches.
Removable drive	A removable hardware component or peripheral device of a computer, such as a zip drive.
RJ-45	Resembling a standard phone connector, an RJ-45 connector is twice as wide (with eight wires) and hooks up computers to local area networks (LANs) or phones with multiple lines.
Scan	To examine items in a file in sequence to find those that meet a particular criteria.
Scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
Secure Password Authentication	An authentication process, which can protect communications, using for example, encryption and challenge/response mechanisms.
Secure Socket Layer (SSL)	Secure Socket Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Sender	The person who is sending an email message to another person or entity.
Server	A program that provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers.
Signature	*See* virus signature.
SMTP	Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol but uses other protocols to access the messages.
SMTP server	A server that relays email messages to their destinations.
SNMP	Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
SNMP trap	A trap is a programming mechanism that handles errors or other problems on a computer program. An SNMP trap handles errors related to network device monitoring. *See* SNMP.
SOCKS4	A protocol that relays transmission control protocol (TCP) sessions at a firewall host to allow application users transparent access across the firewall.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Spam	Unsolicited email messages meant to promote a product or service.
Spyware	Advertising-supported software that typically installs tracking software in your system, capable of sending information about you to another party. The danger is that users cannot control what the collected data is, or how it is used.
Switch	A device that filters and forwards packets between LAN segments.
Total Solution CD	A CD containing the latest product versions and all the patches applied during the previous quarter. The Total Solution CD is available to all Trend Micro Premium Support customers.
Traffic	Data flowing between the Internet and your network, both incoming and outgoing.
Traffic Mirroring	Used on network devices such as switches to send a copy of specific network packets that pass one switch port (or an entire VLAN) to a network monitoring connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic such as Threat Discovery Appliance.
Trojan Horse	A malicious program disguised as something benign. A Trojan is an executable program that does not replicate, but instead, resides in a system to perform malicious acts, such as opening a port for an intruder.
True file type	Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Trusted domain	A domain from which your Trend Micro product will always accept messages, without considering whether the message is spam. For example, a company called Dominion, Inc. has a subsidiary called Dominion-Japan, Inc. The dominion.com network always accepts messages from dominion-japan.com, without checking for spam, since the messages are from a known and trusted source.
Trusted host	A server allowed to relay mail through your network because they are trusted to act appropriately and not, for example, relay spam through your network.
URL	Universal Resource Locator—A standard way of specifying the location of an object, typically a web page, in the Internet, for example, *www.trendmicro.com*. The URL maps to an IP address using DNS.
VBscript virus	VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a “Click Here for More Information” button on a web page. A VBscript virus is a virus targeted at the scripts in the HTML code. This enables the virus to reside in web pages and download to a user’s desktop through the user’s browser. *Also see* JavaScript virus.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Virtual Local Area Network (VLAN)	A logical (rather than physical) grouping of devices that constitute a single broadcast domain. You do not identify VLAN members by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. The IEEE 802.1Q standard describes VLANs more thoroughly.
Virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
Virus kit	A template of source code for building and executing a virus, available from the Internet.
Virus signature	A virus signature is a unique string of bits that identifies a specific virus. Virus signatures are stored in the Trend Micro virus pattern file. The Trend Micro scan engine compares code in files, such as the body of an email message, or the content of an HTTP download, to the signatures in the pattern file. If the scan engine finds a match, they will detect and act upon the virus (for example, cleaned, deleted, or quarantined) according to your security policy.
Virus writer	Another name for a computer hacker, someone who writes virus code.

TABLE B-1. Glossary of Terms (Continued)

TERM	DEFINITION
Web	The World Wide Web, also called the web or the Internet.
Wildcard	A term used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a "wildcard," can be used for any number or suit in the card deck.
Worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.
Zip file	A compressed archive (in other words, “zip file") from one or more files using an archiving program such as WinZip.

Index

U

V

W