TREND MICRO™

Threat Discovery Appliance[2]

Administrator's Guide

Endpoint Security

Network Security

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

www.trendmicro.com/download/documentation/

Release Date: June 2009

Document Part No: APEM23577/80304

Patents Pending

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

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

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

www.trendmicrcom/download/documentation/rating.asp

Contents

Preface

Documentation x
Audience x
Document Conventions xi

Chapter 1: Introducing Threat Discovery Appliance

Understanding Threat Discovery Appliance 1-2
Threat Discovery Appliance Features 1-2
- Virus Scan Engine 1-3
- Network Virus Scan 1-4
- Network Content Inspection Engine 1-4
- Network Content Correlation Engine 1-4
- Potential Risk File Capture 1-4
- Offline Monitoring 1-5
- Multiple Protocol Support 1-5
- Product Integration 1-6

What's New in This Release 1-6
- Hardware 1-6
- Software 1-6
- Configuration 1-7
- Logs 1-8
- Integration 1-8

Chapter 2: Mounting Threat Discovery Appliance

System Requirements 2-2
- Hardware Requirements 2-3
- Application Requirements 2-4

Device Details 2-5
Configuration Settings 2-5
Power Supplies 2-5
Rack Mounting 2-7

General Installation 2-8
Before You Begin 2-8
Important Safety Information 2-8
Recommended Tools and Supplies 2-9
Rack Kit Contents 2-10

Mounting the Device 2-11

Using the Liquid Crystal Display Module (LCM) 2-27
Reading the LCD 2-27

Chapter 3: Getting Started

Network Settings 3-2

Product Console 3-3
Changing the Product Console Password 3-4

Configuring IP Address Settings 3-4

Setting System Time 3-6

Configuring Proxy Settings 3-7

Activating or Renewing the Product License 3-8

Updating Components 3-9
Configuring Update Settings 3-11

Chapter 4: Configuring Device Settings

Network Configuration 4-2
Adding Monitored Networks 4-2
Removing Monitored Network Groups 4-4
Adding Registered Domains 4-4
Removing Registered Domains 4-5

Adding Registered Services 4-6
Removing Registered Services 4-6
Backing Up Network Configuration Settings 4-7
Importing Network Configuration Settings 4-8

Detections 4-9
Configuring Threat Detections 4-9
Configuring Application Filters 4-9
Saving Detected Files 4-13
Configuring the Detection Exclusion List 4-15

Threshold Settings 4-18

Configuring Threat Management Services Settings 4-20

Configuring LeakProof™ Settings 4-22

Product Integration 4-23
Registering to Mitigation Devices 4-23
Registering to Control Manager 4-25

Backup/Restore 4-28
Backing Up Device Configuration Settings 4-28
Restoring Device Configuration Settings 4-29
Resetting Device Settings 4-30

Updating the Firmware 4-31

System Maintenance 4-33
Shutting Down Threat Discovery Appliance 4-33
Restarting Threat Discovery Appliance Services 4-34
Restarting Threat Discovery Appliance 4-34

Chapter 5: Viewing and Analyzing Information

Status Indicators 5-2
Risk Meter 5-2
Appliance Health 5-2
Network Flow 5-3

Viewing the Summary Screen 5-4
Detections in Past 24 Hours 5-5
Recent Alerts 5-6

Using Notifications 5-8
Configuring Delivery Options 5-8
Configuring Potential Security Risk Notifications 5-10
Disabling Potential Security Risk Notifications 5-11
Configuring Known Security Risk Notifications 5-12
Disabling Known Security Risk Notifications 5-13
Configuring High Risk Client Notification 5-13
Disabling High Risk Client Notifications 5-15
Configuring High Network Traffic Usage Notifications 5-15
Disabling High Network Traffic Usage Notifications 5-17

Viewing Logs and Reports 5-18
Reports 5-18
Configuring Report Delivery Settings 5-23
Disabling Report Delivery Notifications 5-23

Logs 5-24

Chapter 6: Preconfiguration and Rescue

Using the Preconfiguration Console 6-2
Entering the Preconfiguration Console 6-2
Preconfiguration Console Overview 6-4
Viewing Device Information and Status 6-6
Configuring Device Settings 6-7
Modifying Interface Settings 6-9
Performing System Tasks 6-11
Viewing the System Logs 6-20
Changing the Root Password 6-21
Logging off from the Preconfiguration Console 6-22

Rescuing Threat Discovery Appliance 6-25
Application Rescue Overview 6-25

Chapter 7: FAQs and Technical Support

Frequently Asked Questions (FAQs) 7-2
Installation 7-2
Activation 7-2
Configuration 7-2

Updating the Device 7-4
Logs 7-4
Documentation 7-5

Trend Micro Technical Support 7-6
Contacting Trend Micro 7-6
The Trend Micro Security Information Center 7-6
Contacting Technical Support 7-8
The Trend Micro Knowledge Base 7-8
Sending Suspicious Files to Trend Micro 7-9
About TrendLabs 7-9

Appendix A: Deploying Threat Discovery Appliance

Deployment Considerations A-2

Deployment Scenarios A-2
Single Port A-3
Dual Port A-4
Network TAP A-5
Redundant Networks A-7
Specific VLANs A-8
Remote Port or VLAN Mirroring A-8
Mirroring Trunk Links A-9

Appendix B: Glossary

Index

Preface

Welcome to the *Trend Micro™ Threat Discovery Appliance Administrator's Guide*. This manual contains information about device installation and product settings.

This preface discusses the following topics:

- *Documentation* on page x
- *Audience* on page x
- *Document Conventions* on page xi

Documentation

The Trend Micro™ Threat Discovery Appliance documentation consists of the following:

- **Quick Start Guide**—Helps you set up Threat Discovery Appliance and connect it to your network.
- **Administrator's Guide**—Helps with installation and configuration of all product settings.
- **Online Help**—Helps you configure all features through the user interface. To access the online help, open the product console and then click the help icon ().
- **Readme File**—Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.
- **License Agreement**—License agreements for Threat Discovery Appliance and third-party applications.

The *Quick Start Guide*, *Administrator's Guide*, and readme file are available in the Threat Discovery Appliance Solutions CD and at:

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

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 I-1. Document conventions described

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 other user interface items
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Information that you need to know to configure the product
Tip:	Trend Micro recommendations or information that will help you with the product
WARNING!	Trend Micro reminders on actions or configurations to avoid

Chapter 1

Introducing Threat Discovery Appliance

This chapter introduces Trend Micro™ Threat Discovery Appliance features, capabilities, and technology.

The topics discussed in this chapter are:

- *Understanding Threat Discovery Appliance* on page 1-2
- *Threat Discovery Appliance Features* on page 1-2
- *What's New in This Release* on page 1-6

Understanding Threat Discovery Appliance

Trend Micro™ Threat Discovery Appliance is a next-generation network monitoring device 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).

The device delivers high-performance throughput and availability and provides critical security information, alerts, and reports to IT administrators. Trend Micro Control Manager™ can manage the Threat Discovery Appliance device.

This version of Threat Discovery Appliance is a stand-alone device. However, to better protect your network, Trend Micro recommends integrating Threat Discovery Appliance with Trend Micro™ Network VirusWall™ Enforcer or Trend Micro™ LeakProof™.

Additionally, you can register to and use Trend Micro™ Threat Management Services. Through these services, Trend Micro can assess Threat Discovery Appliance logs and send weekly reports with detailed information, including recommended actions.

Threat Discovery Appliance Features

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

- Virus Scan Engine
- Network Virus Scan
- Network Content Inspection Engine
- Network Content Correlation Engine
- Potential Risk File Capture
- Offline Monitoring
- Multiple Protocol Support
- Product Integration

Virus Scan Engine

The Threat Discovery Appliance 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 *Updating Components* on page 3-9).

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. This device monitors network packets and triggers events that can indicate an attack against a network. The device can also scan traffic in specific network segments.

Network Content Inspection Engine

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

Network Content Correlation Engine

Network Content Correlation Engine is the program module used by the device 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.

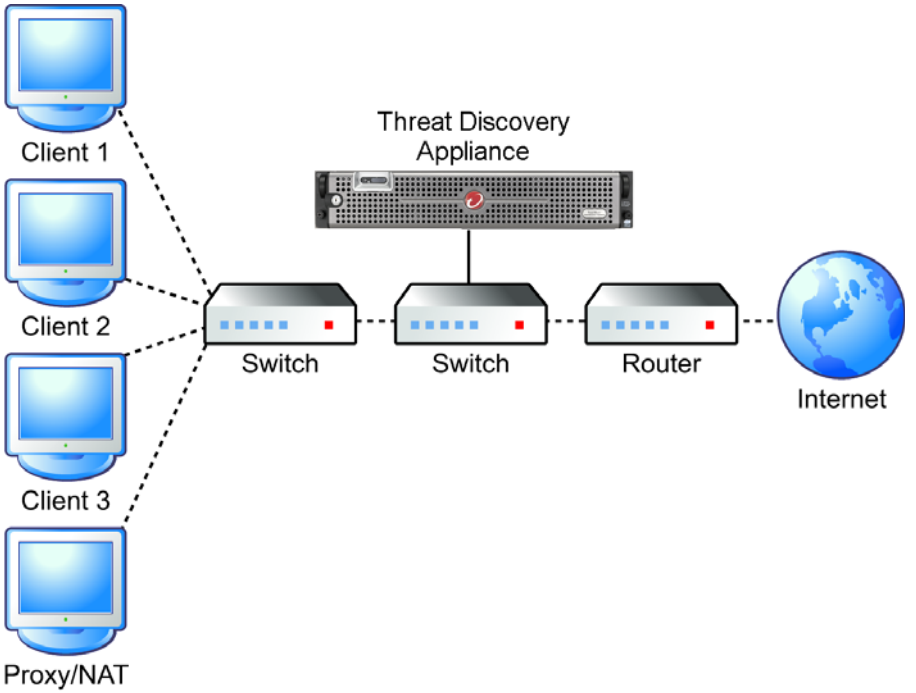
Potential Risk File Capture

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 the file in the physical storage of the device. 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. The device monitors the network traffic by connecting to the mirror port on a switch for minimal or no network interruption.

FIGURE 1-1. Threat Discovery Appliance deployment architecture



Multiple Protocol Support

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

Product Integration

Integration with Mitigation Servers

Threat Discovery Appliance integrates with mitigation devices such as Trend Micro™ Network VirusWall™ Enforcer and Trend Micro™ Threat Mitigator, which analyze, mitigate, and block infected computers.

Integration with 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.

What's New in This Release

Here are the new features released for this version.

Hardware

VMware™ ESX™ or ESXi server support

Trend Micro provides the option of using the hardware provided by Trend Micro or using the hardware supported by VMware ESX or ESXi server that best suits your needs.

Enhanced Multiple Port Scan

Threat Discovery Appliance can simultaneously monitor traffic on six separate networks using a dedicated port for each network.

Software

Remote System Maintenance

Shut down, or restart the device or service from the product console.

Increased Simultaneous Connection Capacity

Threat Discovery Appliance supports more concurrent connections.

Network Flow Indicator

Network Flow indicator displays device capacity of scanning network traffic.

Configuration

Setup Guide

Threat Discovery Appliance provided a step by step guide on configuring device settings. Access the setup guide from the Summary screen beside the **Log Off** button.

Outbreak Containment Services

Outbreak Containment Services blocks and disconnects malware activities that have the potential to cause an outbreak.

Detection Exclusion List

The Detection Exclusion List includes servers or computers that:

- do not need to log potential security threats.
- should not be blocked by Outbreak Containment Services.

IP address range in Mitigation Settings

Assign an IP address range to a specific mitigation device.

Mitigation Exclusion List

Add the IP addresses to exclude the servers or computers from mitigation requests sent to mitigation devices.

Enhanced Mitigation Capability

Trend Micro enhanced the Threat Discovery Appliance mitigation capability to target specific kinds of malware that query domain names that Trend Micro considers suspicious and malware that propagate through Windows fileshare (SMB) protocols.

Logs

Additional Criteria in Detection Log Query

Trend Micro added more filters including Outbreak Containment Services, Mitigation, computer name, and Active Directory Domain name and account for Detection log query.

Threat Detail Information

Trend Micro added the Detection Type, Mitigation, Outbreak Containment Service, and Active Directory Domain Name and Account as additional threat details.

Integration

Mitigation Servers

Threat Discovery Appliance integrates with mitigation devices such as Trend Micro™ Network VirusWall™ Enforcer and Trend Micro™ Threat Mitigator that analyze, mitigate, and block infected computers.

Threat Management Services

Threat Discovery Appliance added real time transmission of detection on malware that have the potential to cause an outbreak to provide better monitoring services.

LeakProof™

Threat Discovery Appliance works with Trend Micro™ LeakProof™ servers to monitor information leakage across segments and throughout the network.

Chapter 2

Mounting Threat Discovery Appliance

This chapter describes the Trend Micro™ Threat Discovery Appliance device and provides instructions on how to physically mount the device.

The topics discussed in this chapter are:

- *System Requirements* on page 2-2
- *Device Details* on page 2-5
- *General Installation* on page 2-8
- *Mounting the Device* on page 2-11
- *Using the Liquid Crystal Display Module (LCM)* on page 2-27

System Requirements

To deploy and configure Trend Micro™ Threat Discovery Appliance, you need the following:

Hardware Requirements:

- Any desktop/notebook computer with an Ethernet and serial port
- Ethernet cable

Application Requirements:

- SSH communications application
- Serial communications application
- Microsoft™ Internet Explorer™ 6.0 or 7.0

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

- Microsoft Virtual Machine™ 5.0 or Sun™ Microsystems Java™ Runtime Environment (JRE) 1.4 or later
- (Optional) Trend Micro Control Manager™ 5.0

For detailed information on the device requirements, refer to *Hardware Requirements* on page 2-3 and *Application Requirements* on page 2-4.

Hardware Requirements

To configure the device settings using the Preconfiguration Console (see *Using the Preconfiguration Console* on page 6-2), refer to *System Requirements* on page 2-2.

TABLE 2-1. Minimum hardware requirements

HARDWARE	DETAILS
Any desktop/notebook computer with an Ethernet and serial port	The computer must have an IP address in the same subnet as Threat Discovery Appliance. By default, VMware assigns the Threat Discovery Appliance IP address. To change IP address settings, refer to *Configuring Device Settings* on page 6-7.
General Ethernet cable	Connect the configuration computer to the Threat Discovery Appliance management port using a general Ethernet cable. From the management port, you can perform initial configuration or re-install the application files.

Application Requirements

Table 2-2 lists the minimum application requirements to access the product console interfaces.

TABLE 2-2. Minimum application requirements

APPLICATION	DETAILS
Serial communications application	To perform initial configuration, use a serial communications application, such as HyperTerminal, when you connect to the console port (refer to the *Threat Discovery Appliance Quick Start Guide)*. Use the following settings: Port: depends on the port you are using Baud rate: 115200 Date: 8 bit Parity: none Stop: 1 bit Flow control: none
Internet Explorer	To access the product console, which allows you to configure all Threat Discovery Appliance settings, use Internet Explorer 6.0 or 7.0. Using the management port IP address you set during initial configuration, type the following URL (refer to the *Threat Discovery Appliance Quick Start Guide)*: `https://[IP Address]`

Device Details

This section provides information on the Threat Discovery Appliance hardware.

Configuration Settings

Threat Discovery Appliance has two hard disks. Each hard disk has 300GB disk space. The primary hard disk is used to store device information, programs, and configuration settings. The primary hard disk has two partitions. The first partition is the primary partition and the secondary partition is for failover. Threat Discovery Appliance uses the secondary hard disk to store logs.

Power Supplies

Threat Discovery Appliance provides two power supplies, the first is the primary power supply and the second is for back up. *Table 2-3* provides specifications for the power supplies.

TABLE 2-3. Power supply specifications

ITEM	DETAILS
Size	265.00x101.00x84.00 (mm)
AC INPUT	100-240V 50-60Hz 10A (MAX)
DC OUTPUT	750W (MAX)

Powering Off

Table 2-4 provides a summary of the different methods you can use to power off Threat Discovery Appliance.

TABLE 2-4. Powering off the device

ACTION	WHEN DEVICE IS TURNED ON
Pressing the power button (briefly)	Threat Discovery Appliance shuts down all applications and powers off normally. This method takes about 30 seconds.
Pressing and holding the power button (5 seconds or longer)	Threat Discovery Appliance immediately shuts down. **WARNING! Using this method might cause some loss of data.**

Threat Discovery Appliance uses a CPU with the specifications listed in *Table 2-5*.

TABLE 2-5. CPU specifications

ITEM	DETAILS
CPU Model	Quad-Core Intel® Xeon® Processor X5355 x 2
Front side bus	1333MHz
BIOS	Phoenix technologies ROM BIOS Plus

Note: If you encounter hardware issues, contact your support provider.

Rack Mounting

Your device is safety-certified as a free-standing unit and as a component for use in a Trend Micro rack cabinet using the customer rack kit. The installation of your device and rack kit in any other rack cabinet has not been approved by any safety agencies. It is your responsibility to ensure that the final combination of device and rack complies with all applicable safety standards and local electric code requirements. Trend Micro disclaims all liability and warranties in connection with such combinations.

Devices are considered to be components in a rack. Thus, "component" refers to any device as well as to various peripherals or supporting hardware.

WARNING! **Before installing devices in a rack, install front and side stabilizers on stand-alone racks or the front stabilizer on racks joined to other racks. Failure to install stabilizers accordingly before installing devices in a rack could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizer(s) before installing components in the rack.**

After installing device/components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.

General Installation

This guide provides instructions for trained service technicians installing one or more devices in a rack cabinet. You can install the RapidRails™ configuration without tools in manufacturer's rack cabinets that have square holes; and you can install the VersaRails™ configuration in most industry-standard rack cabinets that have square or round holes. Each device requires one rack kit for installation in the rack cabinet.

Note: For instructions on installing the device itself, see *Step 5: Installing the Device in the Rack* on page 2-20.

Before You Begin

Before you begin installing your device in the rack, carefully read the Safety Sheet that comes with this device.

WARNING! **When installing multiple devices in a rack, complete all of the procedures for the current device before attempting to install the next device.**

Rack cabinets can be extremely heavy and move easily on their casters. They do not have brakes. Use extreme caution while moving the rack cabinet. Retract the leveling feet when relocating the rack cabinet. Avoid long or steep inclines or ramps where loss of cabinet control may occur. Extend the leveling feet for support and to prevent the cabinet from rolling.

Important Safety Information

Observe the safety precautions in the following subsections when installing your device in the rack.

WARNING! **You must strictly follow the procedures in this document to protect yourself as well as others who may be involved. Your device may be very large and heavy and proper preparation and planning is important to prevent injury to yourself and to others. This precaution becomes increasingly important when installing devices high up in the rack.**

Do not install rack kit components designed for another device. Use only the rack kit for your device. Using the rack kit for another device may result in damage to the device and personal injury to yourself and to others.

Recommended Tools and Supplies

You may need the following items to install the device in a four-post rack cabinet:

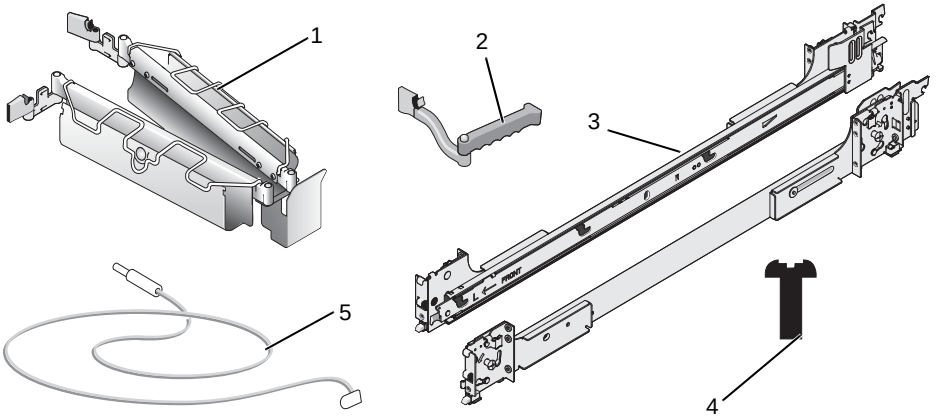
- #2 Phillips screwdriver
- Masking tape or a felt-tip pen, for use in marking the mounting holes to be used

Rack Kit Contents

- One pair of slide assemblies
- One cable-management arm
- One cable-management arm retainer
- One status indicator cable (if applicable)
- Eight 10-32 x 0.5-inch flange-head Phillips screws

Note: Identify the nonnon-metricmetric screws described in illustrations and in procedural steps by the size and number of threads per inch. For example, a #10 Phillips-head screw with 32 threads per inch is a 10-32 screw.

FIGURE 2-1. Rack Kit Contents



1	cable-management arm	2	cable-management arm retainer	3	slide assemblies (2)
4	10-32 x 0.5-inch flange-head Phillips screws (8)	5	status indicator cable (if applicable)		

Mounting the Device

Installing a rack kit involves performing the following tasks (described in detail in subsequent sections):

Step 1: Removing the Rack Doors on page 2-11

Step 2: Marking the Rack on page 2-11

Step 3: Configuring the Sliding Rail Assemblies on page 2-14

Step 4: Installing the Mounting Rails in the Rack on page 2-16

- *Installing the RapidRails Mounting Rails* on page 2-16
- *Installing the VersaRails Mounting Rails* on page 2-19

Step 5: Installing the Device in the Rack on page 2-20

Step 6: Installing the Cable-Management Arm on page 2-23

Step 7: Routing Cables on page 2-24

Step 8: Attaching the Cable-Management Arm Retainer on page 2-25

Step 9: Replacing the Rack Doors on page 2-27

Step 1: Removing the Rack Doors

See the procedures for removing doors in the documentation provided with your rack cabinet.

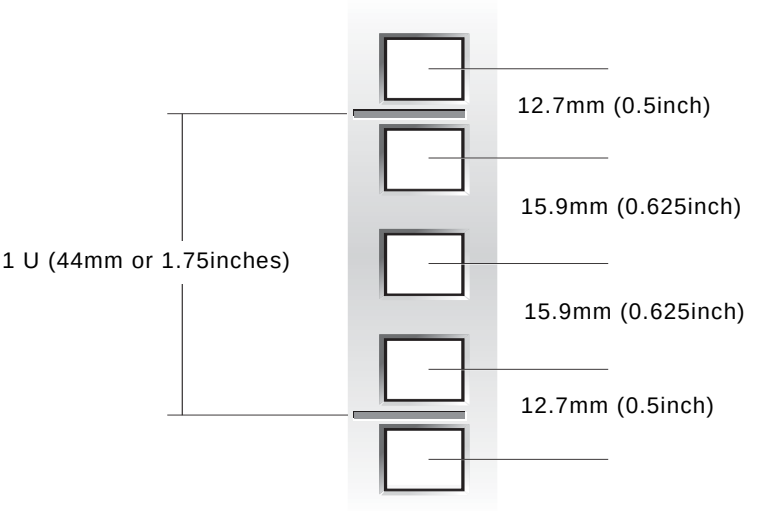
WARNING! **Because of the size and weight of the rack cabinet doors, never attempt to remove or install them by yourself. Also, ensure that you store the doors where they will not injure someone if the doors accidently fall over.**

Step 2: Marking the Rack

For a 2-U device, you must allow 2 U (88mm, or 3.5 inches) of vertical space for each device you install in the rack.

Tip: If you are installing more than one device, ensure that you install the mounting rails in a way that allows you to install the first device in the lowest available position in the rack.

FIGURE 2-2. One Rack Unit



Rack cabinets that meet EIA-310 standards have an alternating pattern of three holes per rack unit with center-to-center hole spacing (beginning at the top hole of a 1-U space) of 15.9mm, 15.9mm, and 12.7mm (0.625inch, 0.625inch, and 0.5inch) for the front and back vertical rails (see *Figure 2-2*). Rack cabinets may have round or square holes.

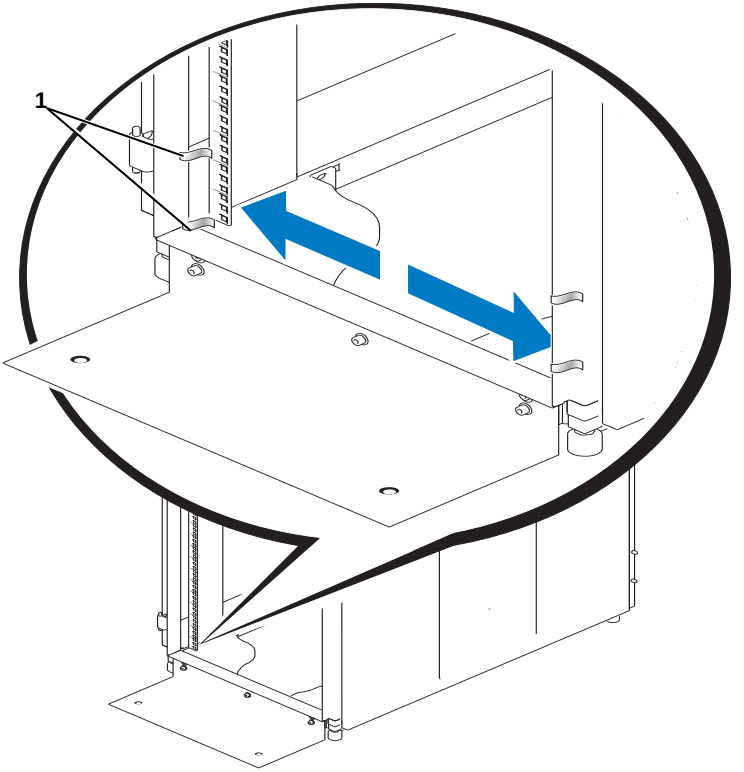
Note: The vertical rails may be marked by horizontal lines and numbers in 1-U increments.

To mark the rack:

1. Place a mark (or tape) on the rack's front vertical rails where you will place the device.

   The bottom of each 1-U space is at the middle of the narrowest metal area between holes (marked with a horizontal line on some rack cabinets, see *Figure 2-3*).

FIGURE 2-3. Marking the Vertical Rails



1 marks on vertical rail (2)

2. Place a mark 88mm (3.5inches) above the original mark you made (or count up three holes in a rack that meets EIA-310 standards) and mark the rack's front

vertical rails with a felt-tipped pen or masking tape (if you counted holes, place a mark just above the top hole).

Step 3: Configuring the Sliding Rail Assemblies

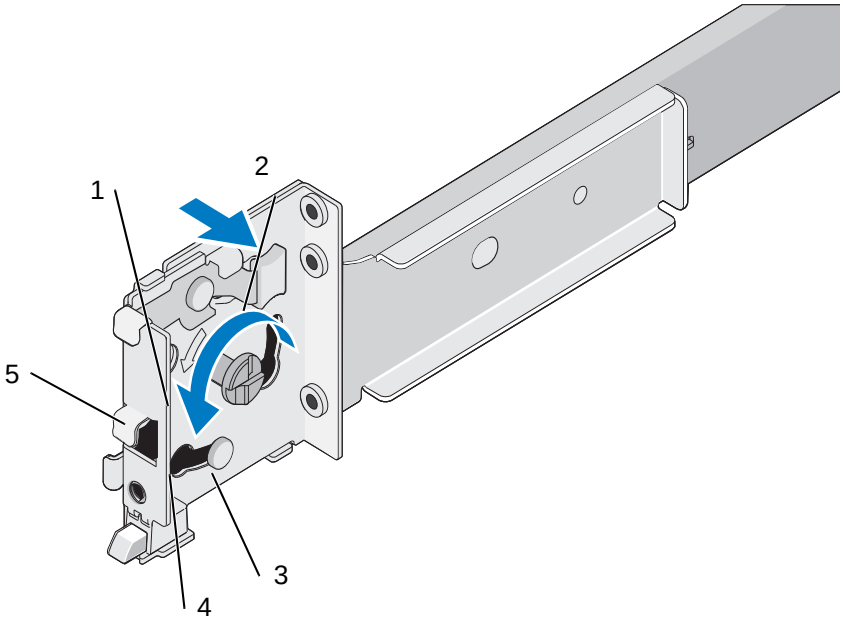
The sliding rail assembly has a rotating mounting bracket at each end of the rail. The position of the bracket determines whether the rail assembly is used as a RapidRail or a VersaRail. The RapidRail side of the bracket has a hook and a latch that secure it to the vertical rail. The VersaRail side of the bracket has three holes and uses screws to attach it to the vertical rail.

Note: The rack kit ships with the slide assemblies in the RapidRails configuration.

To change from one type to the other type of rail assembly:

1. Lift the blue lever on the rotating mounting bracket (see *Figure 2-4*).

FIGURE 2-4. Changing the Position of the Rotating Mounting Bracket



1	rotating bracket	2	release lever	3	shoulder standoffs (2)
4	notches (2)	5	mounting-bracket flange (RapidRails version shown)		

2. Rotate the bracket and slide it up off of the two shoulder standoffs.
3. Continue to rotate the bracket 180 degrees until you can set the notches back over the shoulder standoffs.
4. Rotate the bracket in the opposite direction until the bracket clicks into place.

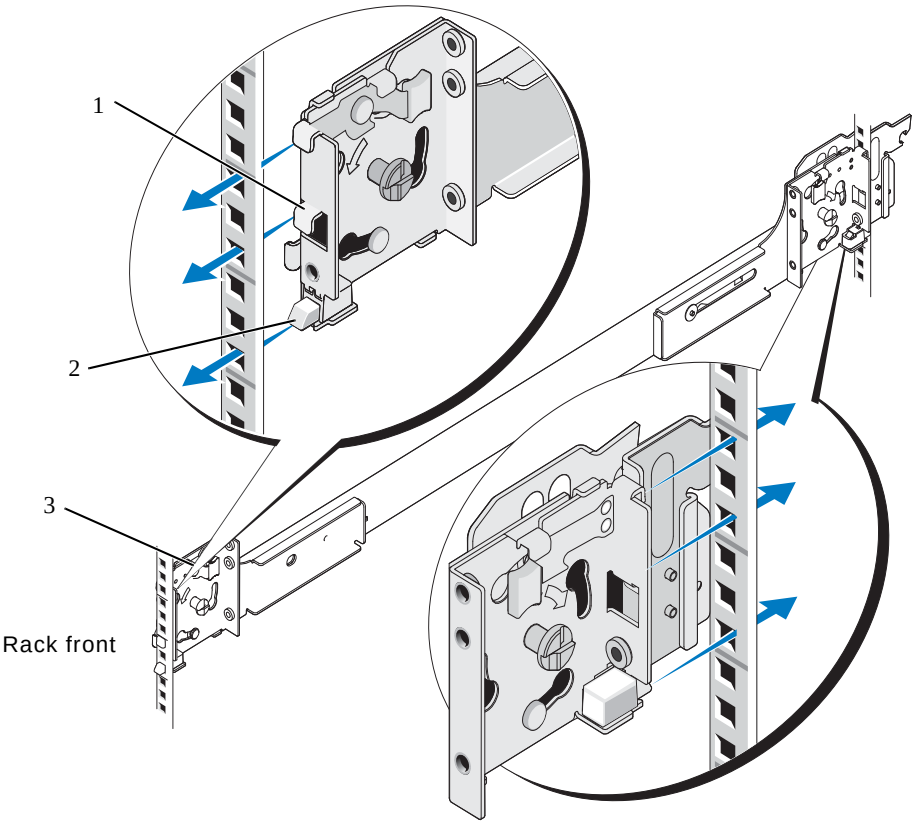
Step 4: Installing the Mounting Rails in the Rack

Installing the RapidRails Mounting Rails

1. At the front of the rack cabinet, position one of the mounting rails so that its mounting-bracket flange fits between the marks or tape you placed (or numbered locations) on the vertical rails in *Step 2: Marking the Rack* on page 2-11 (see *Figure 2-5*).

   The top mounting hook on the front mounting-bracket flange should enter the top hole between the marks you made on the vertical rails.

FIGURE 2-5. Installing RapidRails Mounting Rails



1 mounting hooks (4) 2 push buttons (2) 3 mounting rails (2)

Note: Ensure that you fix the rotating mounting brackets on the slide assemblies in the RapidRail configuration.

2. Push the mounting rail forward until the mounting hooks enter their square holes. Then push down on the mounting-bracket flange until the mounting hooks seat and the push button pops out and clicks (see *Figure 2-5*).

3. At the back of the cabinet, pull back on the mounting-bracket flange until the mounting hooks enter their square holes. Then push down on the flange until the mounting hooks seat and the push button pops out and clicks.
4. Repeat Steps 1 to 3 for the mounting rail on the other side of the rack.

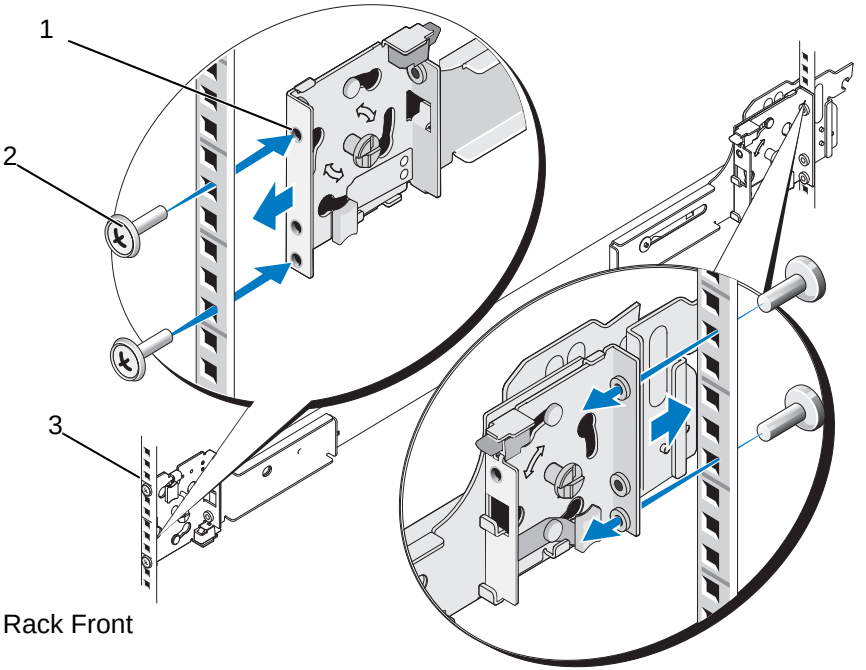
Note: Ensure that you fix the mounting rails at the same vertical position on both sides of the rack (see *Figure 2-5*).

Installing the VersaRails Mounting Rails

1. At the front of the rack cabinet, position one of the mounting rails so that its mounting-bracket flange fits between the marks you placed (or numbered locations) on the vertical rails in *Step 2: Marking the Rack* on page 2-11 (see *Figure 2-6*).

   The three holes on the front of the mounting-bracket flange should align with the holes between the marks you made on the front vertical rail.

FIGURE 2-6. Installing VersaRails Mounting Rails



1 mounting-bracket flange

2 10-32 x 0.5-inch flange-head Phillips screws (4 per mounting rail)

3 mounting rails (2)

Note: Ensure that the rotating mounting brackets on the slide assemblies are in the VersaRail configuration (see *Figure 2-6*).

2. Install two 10-32 x 0.5-inch flange-head Phillips screws in the upper and lower holes in the mounting-bracket flange to secure the mounting rail to the front vertical rail.
3. At the back of the cabinet, pull back on the mounting-bracket flange until the mounting holes align with their respective holes on the back vertical rail.
4. Install two 10-32 x 0.5-inch flange-head Phillips screws in the upper and lower holes in the mounting-bracket flange to secure the mounting rail to the back vertical rail.
5. Repeat Steps 1 to 4 for the mounting rail on the other side of the rack.

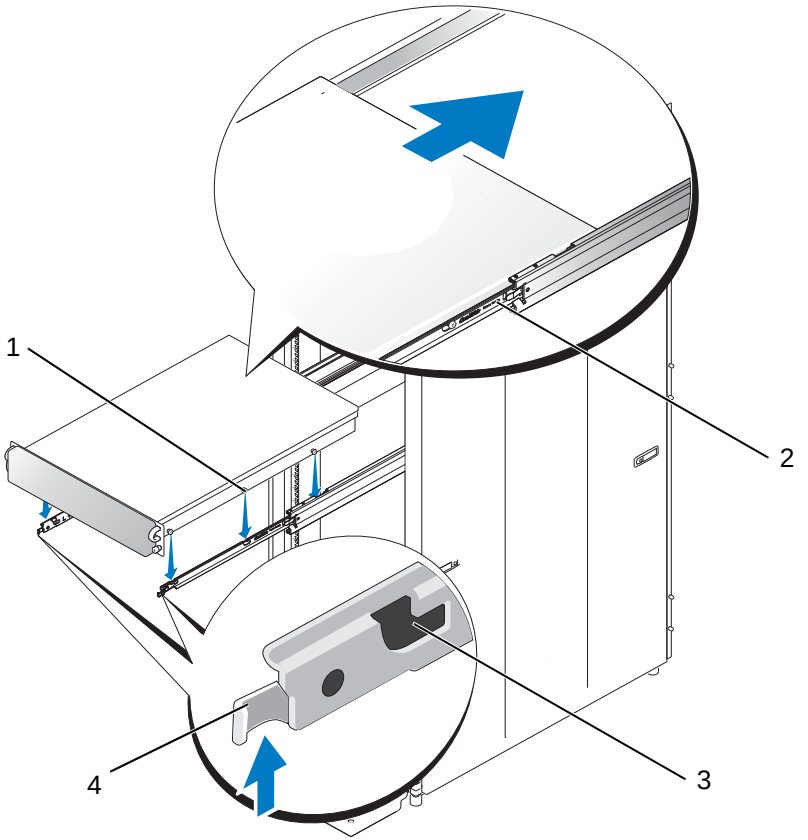
Note: Ensure that you fix the mounting rails at the same vertical position on both sides of the rack (see *Figure 2-6*).

Step 5: Installing the Device in the Rack

1. Pull the two inner slide rails out of the rack until they lock in the fully extended position.
2. Lift the device into position above the extended slides.

   The three shoulder screws on the sides of the device fit into the corresponding J-slots (see details on *Figure 2-7*) on the inner slide assemblies.

FIGURE 2-7. Installing the Device in the Rack



1 shoulder screws (6) 2 slide-release latch 3 J slots (6)
4 front release latch

Tip: If you are installing more than one device, install the first device in the lowest available position in the rack.

3. Lower the back of the device while aligning the back shoulder screws on the sides of the device with the back J-slots on the slide assemblies.
4. Engage the back shoulder screws into their respective J-slots.
5. Lower the front of the device and fit the middle and front shoulder screws into the J-slots in the slide assemblies.
6. The device release latch at the front of the inner slide rail will snap back as the shoulder screw passes into the front slot.

Note: Use this device release latch to remove the device from the slide assemblies (see *Figure 2-7*).

---

7. Press the slide-release latch on the outside of each inner slide and then push the device into the rack.
8. Install the cable-management arm. See *Step 6: Installing the Cable-Management Arm* on page 2-23.
9. Tighten the thumbscrews on the rack front panel to secure the slide assemblies to the rack.

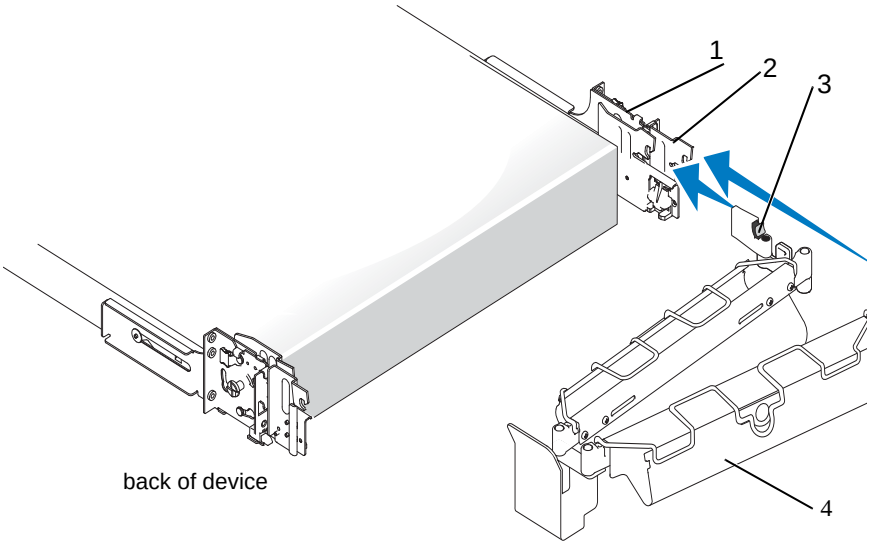
To remove the device from the rack:

1. Turn off the device and attached peripherals, and disconnect the device from the electrical outlet.
2. Remove the I/O cable connectors and power cable connectors from their respective connectors on the device back panel.
3. Loosen the thumbscrews on each side of the front chassis panel that secures the device to the rack.
4. Pull the device out of the rack until it stops because of the safety catch.
5. Pull up on the front release latch on each rail to disengage the safety catch (see *Figure 2-7*) and slide the device forward.
6. Pull the device completely out of the rack.

Step 6: Installing the Cable-Management Arm

1. Fit the latch on the front end of the cable-management arm onto the bracket on the end of the mounting rail until the latch clicks (see *Figure 2-8*).

FIGURE 2-8. Installing the Cable-Management Arm



1 mounting rails (2) 2 brackets (2) 3 latches (2)
4 cable-management arm

Note: Attach the cable-management arm to either side of the rack cabinet and the cable-management arm retainer at the opposite side.

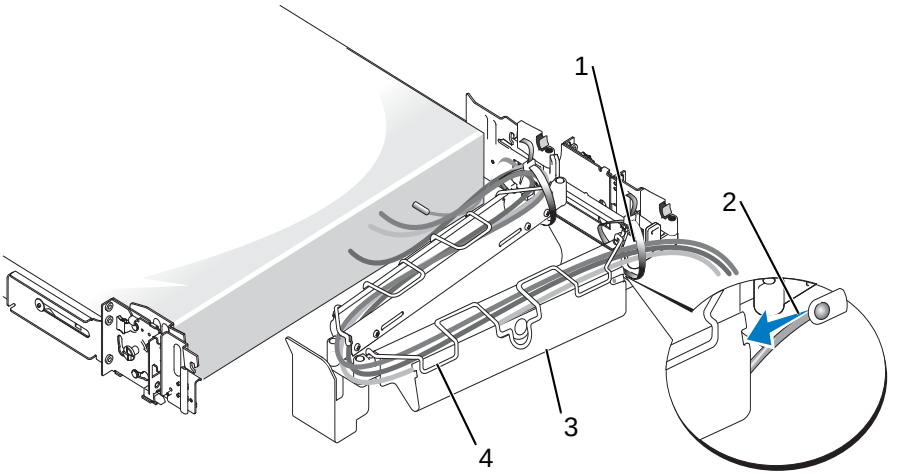
2. Fit the latch on the unattached end of the cable-management arm onto the bracket on the end of the slide assembly until the latch clicks (see *Figure 2-8*).

Note: Connect both ends of the cable-management arm before you begin routing the device cables.

Step 7: Routing Cables

1. Open the wire cable basket on the top of the cable-management arm, to route cables within the arms (see *Figure 2-9*).

FIGURE 2-9. Routing Cables on the Cable-Management Arm



1 tie wraps (2) 2 device status-indicator cable connector 3 cable-management arm

4 wire cable basket

2. If applicable, connect the device status-indicator cable to its connector on the back panel.

   Route the device status-indicator cable through the cable-management arm. Press the LED into the slot at the end of the cable-management arm until it snaps into place.

3. Attach the I/O cable connectors and power cable connectors to their respective connectors on the back panel.

Note: Use the retainer brackets on the back of the power supplies to provide strain relief for the power cables.

4. Route the cables along the bend in the cable-management arm.
5. Adjust the cable slack as needed at the hinge position and secure the cables with the tie wraps (see *Figure 2-9*).
6. Close the cable basket.
7. Slide the device in and out of the rack to verify that the cables are routed correctly and do not bind, stretch, or interfere with the movement of the cable-management arm. Adjust the cable positioning inside the cable management arm as needed.

Note: If you pull the device out to its furthest extension, the slide assemblies will lock in the extended position. To release the lock, press the slide release latch on the side of each slide and then slide the device into the rack.

8. When the cables are routed correctly, push the device fully into the rack.

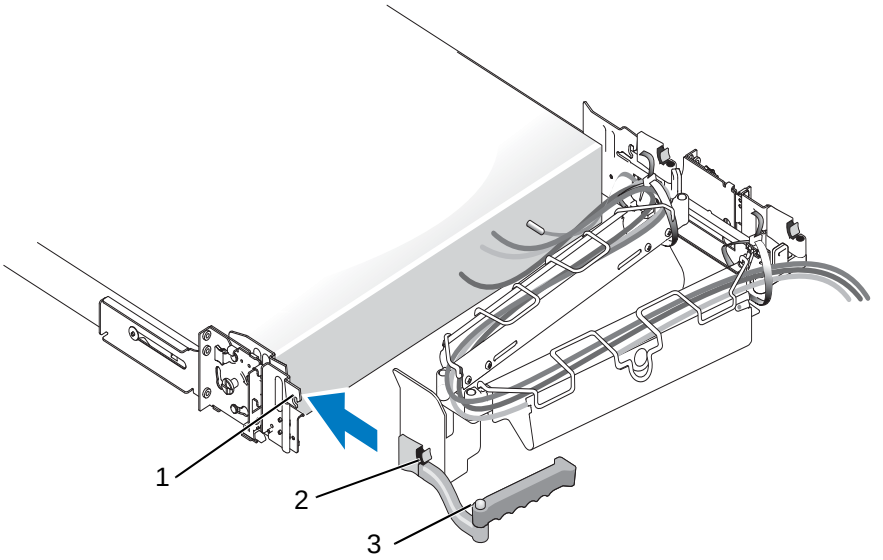
Step 8: Attaching the Cable-Management Arm Retainer

The cable-management arm retainer keeps the cable-management arm in place.

To attach the cable-management arm retainer:

1. Connect the release latch on the cable-management arm retainer to the tab on the outer slide assembly (see *Figure 2-10*).

FIGURE 2-10. Installing the Cable-Management Arm Retainer



1 tab 2 release latch 3 blue button

Note: Attach the cable-management arm retainer to the side opposite of where you attach the cable-management arm.

2. Fold the cable-management arm retainer until it locks into place behind the cable-management arm.

To unlock the cable-management arm retainer:

1. Press the blue button on the cable-management arm retainer while lifting the retainer arm.
2. Rotate the arm of the retainer to an open position.

Step 9: Replacing the Rack Doors

See the procedures for replacing doors in the documentation provided with your rack.

Using the Liquid Crystal Display Module (LCM)

A liquid crystal display module (LCM) is located in the front part of the device. The display module includes the liquid crystal display (LCD) component, which displays the host name and IP address.

Reading the LCD

The LCD shows the following:

- `host name` - the default Threat Discovery Appliance host name
- `192.168.252.1` - the default IP address of the Threat Discovery Appliance management port

Chapter 3

Getting Started

This chapter introduces the settings you need to configure immediately after installing Trend Micro™ Threat Discovery Appliance.

The topics discussed in this chapter are:

- *Network Settings* on page 3-2
- *Product Console* on page 3-3
- *Configuring IP Address Settings* on page 3-4
- *Setting System Time* on page 3-6
- *Configuring Proxy Settings* on page 3-7
- *Activating or Renewing the Product License* on page 3-8
- *Updating Components* on page 3-9

Network Settings

The following format rules apply to Trend Micro™ 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 to 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:

- `255.255.255.0`—Binary format is `11111111.11111111.11111111.00000000`
- `255.255.252.0`—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-based product console through which you can configure all Threat Discovery Appliance settings. This section explains how to access the product console.

To open the product console:

1. From a computer in your network, open Microsoft™ Internet Explorer™ 6.0 or 7.0.
2. Using the managed port IP address you set for Threat Discovery Appliance during initial configuration (refer to the *Threat Discovery Appliance Quick Start Guide*), 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 *Changing the Product Console Password* on page 3-4).

4. Click **Log On**.

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

Changing the Product Console Password

The default Threat Discovery Appliance console password is **admin**. For improved security, Trend Micro recommends periodically changing the product console password.

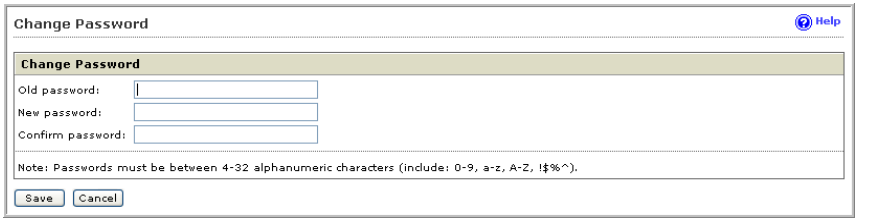
Tip: Passwords should be a mixture of alphanumeric characters such as 0-9, a-z, A-Z, !$%^ and must be 4 to 32 characters long. Avoid words that can be found in the dictionary, names, and dates.

If you lose the password, there is no way to recover it. Contact your support provider (see *Contacting Technical Support* on page 7-8) for assistance in resetting the unknown password.

To change the product console password:

1. Click **Administration** on the main menu. A drop-down menu displays.
2. Click **Password** from the drop-down menu. The Change Password screen displays.

FIGURE 3-1. The Change Password screen



3. Type the current password.
4. Type the new password and confirm it.
5. Click **Save**.

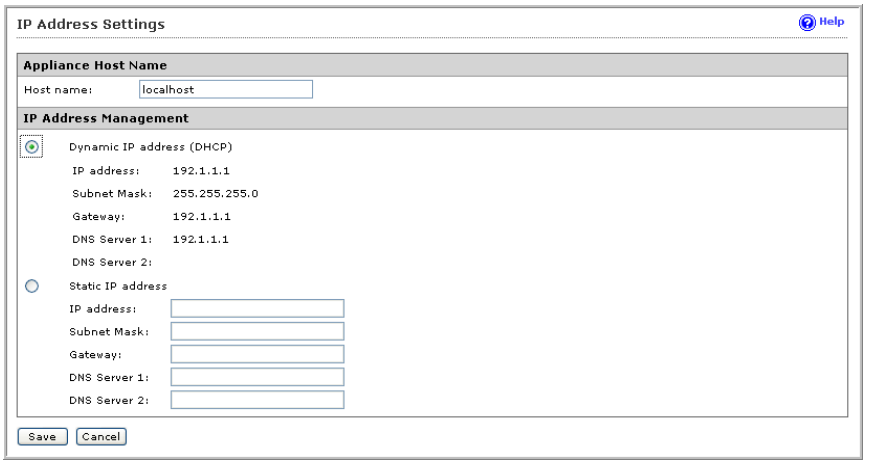
Configuring IP Address Settings

Threat Discovery Appliance is a stand-alone device and requires its own IP address to ensure that the management port can access the product console.

To configure the IP address settings:

1. Click **Administration** on the main menu. A drop-down menu displays.
2. Click **IP Address Settings** from the drop-down menu. The IP Address Settings screen displays.

FIGURE 3-2. The IP Address screen



3. Under **Appliance Host Name**, specify the device host name.
4. Under **IP Address Management**, select the type of IP address to use. If there is a DHCP server in 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** and specify the **IP address**, **Subnet Mask**, **Default gateway**, and **Primary** and **Secondary DNS servers**.

> **Note:** Add the IP address to the SMTP relay list and the host name to the DNS server to ensure that assigned recipients receive the notifications.

5. Click **Save**.

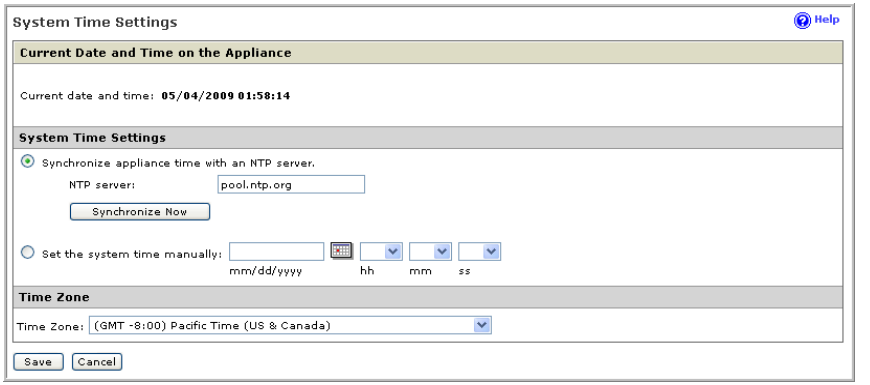
Setting System Time

Synchronize the Threat Discovery Appliance time with the Network Time Protocol (NTP) server, or manually configure the device time.

To set the device system time:

1. Click **Administration** on the main menu. A drop-down menu displays.
2. Click **System Time** from the drop-down menu. The System Time screen displays.

FIGURE 3-3. The System Time Settings screen



3. 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 system time
     i. Type the month, day, and year using the mm/dd/yy format.
     ii. Select the hour, minute, and second.
4. Under **Time zone**, select the appropriate time zone from the list of standard time zones.
5. Click **Save**.

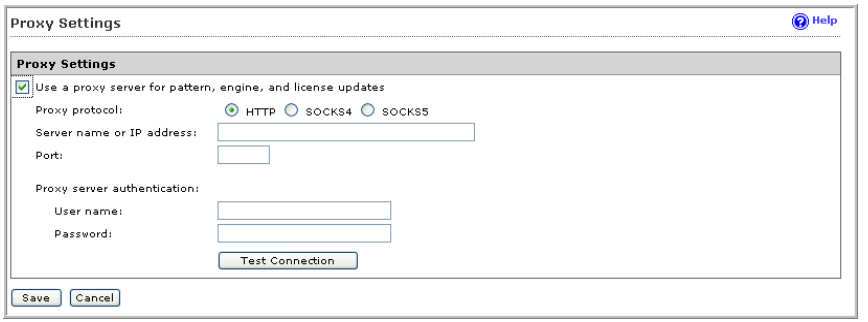
Configuring Proxy Settings

Configure proxy settings to download updates from the Trend Micro ActiveUpdate server or another update source, update the Threat Discovery Appliance license, and query the Trend Micro URL Filtering server.

To configure proxy settings:

1. Click **Administration** on the main menu. A drop-down menu displays.
2. Click **Proxy Settings** from the drop-down menu. The Proxy Settings screen displays.

FIGURE 3-4. The Proxy Settings screen



3. Select the Use **a proxy server for pattern, engine, and license updates** option.
4. Select **HTTP**, **SOCKS4**, or **SOCKS5** for the **Proxy protocol**.
5. 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.
6. If your proxy server requires authentication, type the **User name** and **Password** under **Proxy server authentication**.
7. Click **Save**.

Tip: Click **Test Connection** to verify connection settings.

Activating or Renewing the Product License

To use the functionality of Threat Discovery Appliance, register Threat Discovery Appliance online to the Trend Micro Online Registration Web site and obtain an Activation Code.

Note: An Activation Code has 37 characters (including the hyphens) and looks like: `XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`.

Activate or renew the Activation Code to enable scanning, product updates, and Threat Management Services log transmissions.

To activate/renew a product service license:

1. Click **Administration** on the main menu. A drop-down menu displays.
2. Click **Product License** in the drop-down menu. The Product License screen displays.
3. Under License Information, click **New Activation Code**. The New Activation Code screen displays.
4. Type the new Activation Code and click **Save**.
5. From the Product License Details screen, click **Update Information** to refresh the screen with the new license details and the status of the service. This screen also provides a link to your detailed license available on the Trend Micro Web site.

Updating Components

Download and deploy Threat Discovery Appliance device updates. Threat Discovery Appliance uses these components to scan for and detect network threats. Because Trend Micro regularly creates new component versions, perform regular updates to address the latest Internet threats.

Threat Discovery Appliance provides several methods for updating components:

- Manual update—when you click **Updates > Manual** on the main menu, Threat Discovery Appliance checks to see if any components are out of date and gives you the option to update the components (see *Manual Updates* on page 3-12).

  Note: Threat Discovery Appliance gives you the option of updating on demand. However, you cannot select which components to update.

- 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 3-13). Scheduled update relieves you of the task of manually keeping Threat Discovery Appliance 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.

To help protect your network, Threat Discovery Appliance uses the components in *Table 3-1*.

TABLE 3-1. Threat Discovery Appliance Components

COMPONENT	DESCRIPTION
Virus Scan Engine	Enables Threat Discovery Appliance to scan for viruses and Trojans.
Virus Pattern file	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 by Threat Discovery Appliance 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.
Threat Discovery Appliance Firmware	The program file used by the device. **Tip:** Trend Micro recommends using the Firmware Update screen when updating the firmware.

Update the Threat Discovery Appliance firmware to take advantage of the latest Threat Discovery Appliance features.

To verify that Threat Discovery Appliance has the latest components, perform a manual update. For instructions, see *Manual Updates* on page 3-12.

Note: Restart the device when updating the Threat Discovery Appliance firmware and Network Content Inspection Engine.

Configuring Update Settings

After configuring the device settings, configure the update settings.

To set up initial update configuration, follow the procedures outlined in the following topics:

1. *Configuring Proxy Settings* on page 3-7
2. *Update Source* on page 3-11
3. *Manual Updates* on page 3-12
4. *Scheduled Updates* on page 3-13

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 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:

1. Click **Updates** on the main menu. A drop-down menu displays.
2. Click **Source** from the drop-down menu. The Update Source screen displays.
3. Under **Download Updates From**, select one of the following update sources:
   - **Trend Micro ActiveUpdate server**—the default selection. The Trend Micro ActiveUpdate server is the default standard source for up-to-date 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: The update source must always begin with `"http://"` because Threat Discovery Appliance does not support UNC paths.

4. Specify **Number of retry attempts** and **Retry interval** for unsuccessful updates.
5. Click **Save**.

Manual Updates

Threat Discovery Appliance allows you to perform updates manually or 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:

- **Component**—the component name
- **Current Version**—the version number of each component currently used by the device
- **Latest Version**—the latest version available on the server
- **Last Updated**—the last date and time Threat Discovery Appliance updated the component

To perform manual updates:

1. Click **Updates** on the main menu. A drop-down menu displays.
2. Click **Manual** from the drop-down menu. The Manual Updates screen displays.

Note: Threat Discovery Appliance automatically checks which components need updating. Clicking **Update** prompts Threat Discovery Appliance to update components.

3. Click **Update** to start updating components.

Note: Restart the device after updating the Firmware or Network Content Inspection Engine.

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: To save Internet bandwidth during peak hours, schedule updates during off-peak hours.

To configure scheduled updates:

1. Click **Updates** on the main menu. A drop-down menu displays.
2. Click **Scheduled** from the drop-down menu. The Scheduled Update screen displays.
3. Select the **Enable Scheduled Component Updates** option.
4. 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.

5. Click **Save**.

Chapter 4

Configuring Device Settings

This chapter explains how to configure Trend Micro™ Threat Discovery Appliance settings.

The topics discussed in this chapter are:

- *Network Configuration* on page 4-2
- *Detections* on page 4-9
- *Threshold Settings* on page 4-18
- *Configuring Threat Management Services Settings* on page 4-20
- *Configuring LeakProof™ Settings* on page 4-22
- *Product Integration* on page 4-23
- *Backup/Restore* on page 4-28
- *Updating the Firmware* on page 4-31
- *System Maintenance* on page 4-33

Network Configuration

Network configuration defines and establishes the profile of the network Trend Micro™ Threat Discovery Appliance monitors. To do this, define monitored networks, services provided, and network domains. The Network Content Correlation Engine then uses this information to establish its knowledge of the network to provide better protection results.

Additionally, you can export the network configuration file and import this to another Threat Discovery Appliance.

Adding Monitored Networks

Establish monitored network groups using internal IP addresses to allow Threat Discovery Appliance to determine whether the attacks in the network are internal or external.

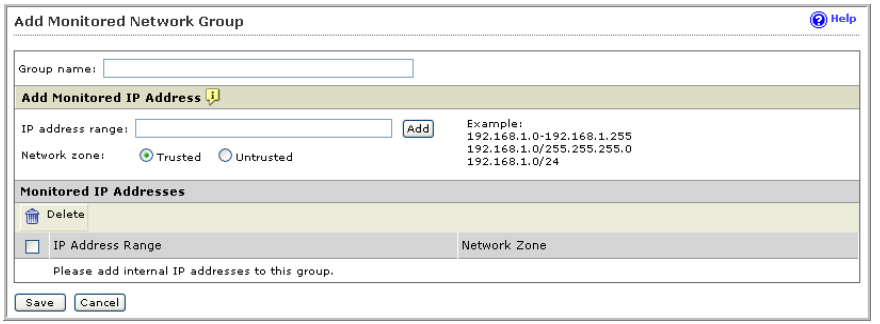
To add monitored networks:

Note: You can add a maximum of 1,000 IP address ranges.

---

1. Click **Network Configuration** on the main menu. A drop-down menu displays.
2. Click **Monitored Network** from the drop-down menu. The Monitored Network screen appears.
3. Click **Add**. The Add Monitored Network Group screen appears.

FIGURE 4-1. The Add Monitored Network Group screen



4. Specify a Group name.

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

---

5. Specify an IP address range in the text box.
   - 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
6. 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.

---

7. Click **Add**.
8. Click **Save**.

Removing Monitored Network Groups

Remove or delete monitored network groups from the list.

To remove monitored network groups:

1. Click **Network Configuration** on the main menu. A drop-down menu displays.
2. Click **Monitored Network** from the drop-down menu. The Monitored Network screen appears.
3. Select the Group Name(s) that you want to remove.
4. Click **Delete**.

Adding 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.

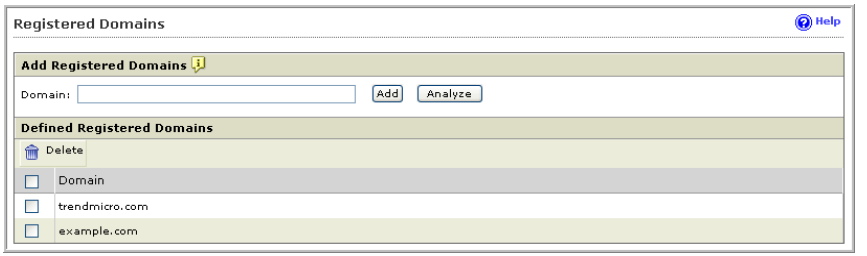
You can add a maximum of 1,000 domains, but add only trusted domains to ensure accuracy of your network profile.

Registered Domains supports suffix matching. This means adding `domain.com`, also adds `one.domain.com, two.domain.com`, and so on

To add registered domains:

1. Click **Network Configuration** on the main menu. A drop-down menu displays.
2. Click **Registered Domains** from the drop-down menu. The Registered Domains screen displays.

FIGURE 4-2. The Registered Domains screen



3. Specify a domain name.

Tip: Clicking **Analyze** displays a list of domains that you can add to the list.

4. Click **Add**.

Removing Registered Domains

Remove or delete registered domains from the list.

To remove registered domains:

1. Click **Network Configuration** on the main menu. A drop-down menu displays.
2. Click **Registered Domains** from the drop-down menu. The Registered Domains screen displays.
3. Select the domain(s) that you want to remove.
4. Click **Delete**.

Adding Registered Services

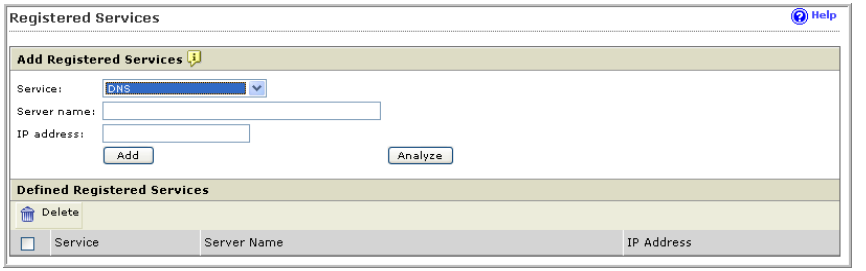
Add different servers for specific services that your organization uses internally or considers trustworthy to establish the network profile. Identifying trusted services in the network ensures detection of unauthorized applications and services.

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:

1. Click **Network Configuration** on the main menu. A drop-down menu displays.
2. Click **Registered Services** from the drop-down menu. The Registered Services screen displays.

FIGURE 4-3. The Registered Services screen



3. Select the service from the drop-down list.

Tip: Clicking **Analyze** displays a list of domains that you can add to the list.

4. (Optional) Specify a server name.
5. Specify an IP address. You cannot add IP address ranges.
6. Click **Add**.

Removing Registered Services

Remove or delete registered services from the list.

To remove registered services:

1. Click **Network Configuration** on the main menu. A drop-down menu displays.
2. Click **Registered Services** from the drop-down menu. The Registered Services screen displays.
3. Select the service(s) you want to delete.
4. Click **Delete**.

Backing Up Network Configuration Settings

Network configuration settings export only the network configuration and detection exclusion list in plain text. This process ensures you have backup settings of the network configuration and makes it easier for you to replicate the settings from one device to another.

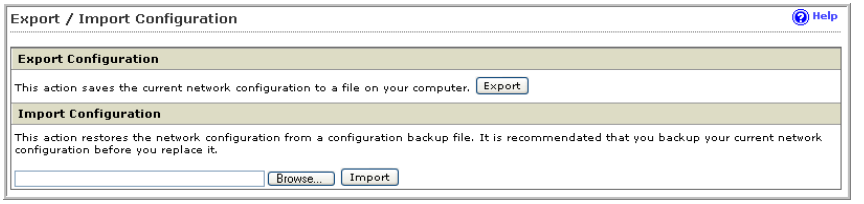
You can open this file using a text editor and add or remove configuration settings. To export/import the device configuration settings, refer to *Backing Up Device Configuration Settings* on page 4-28.

Note: The network configuration file contains only the configurations for the network. However, you can open and modify this file.

To export the network configuration settings:

1. Click **Network Configuration** on the main menu. A drop-down menu displays.
2. Click **Export/Import Configuration** from the drop-down menu. The Export/Import Network Configuration screen displays.

FIGURE 4-4. The Export/Import Configuration screen



3. Under **Export Configuration**, click **Export**. A window appears to open or save the file.
4. Select **Save** and specify the location to save the `.xml` file to.
5. Click **Save**.

Importing Network Configuration Settings

Import the network configuration settings to replicate the settings from one device to another.

To import the network configuration settings:

1. Click **Network Configuration** on the main menu. A drop-down menu displays.
2. Click **Export/Import Configuration** from the drop-down menu. The Export/Import Network Configuration screen displays.

WARNING! Back up network configuration settings by exporting the file before importing a new file.

3. Under **Import Configuration**, click **Browse**. Locate the saved network configuration file and click **ok**.
4. Click **Import**.

Detections

Detections establishes filters and exclusions for the Threat Discovery Appliance network detection features.

Configuring Threat Detections

Configure the Threat Discovery Appliance threat detections feature and Outbreak Containment Services block action to contain an outbreak before it can spread.

Enable or disable the following features.

- **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:

1. Click **Detections** on the main menu. A drop-down menu displays.
2. Click **Threat Detections** from the drop-down menu. The Threat Detections screen displays.
3. Enable the **Enable threat detections** option.
4. Under **Threat Detections**, enable the second **Enable threat detections** option
5. Under Outbreak Containment Services, select the **Enable outbreak detection and block traffic** option.
6. Click **Save**.

Configuring Application Filters

With the variety of software applications, virus/malware infection methods, and files downloaded from the Internet, protect your network by enabling Threat Discovery Appliance Application Filters. Application Filters provide valuable information to help you quickly identify security risks and prevent the spread of malicious code.

Tip: Trend Micro recommends enabling detection for **Instant Messaging**, **P2P Traffic**, and **Streaming Media**.

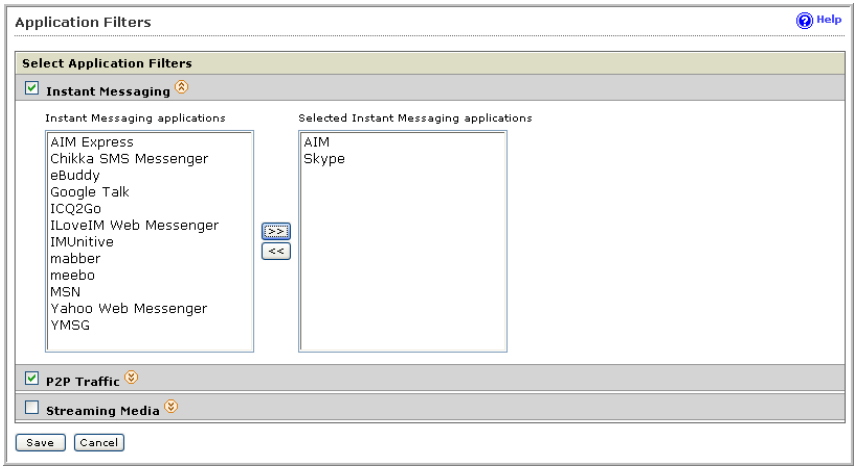
Enable detection for the following protocols:

- **Instant Messaging**—a popular means of communicating and sharing information and files with contacts
- **P2P Traffic**—using peer-to-peer protocol to share files from one computer to another
- **Streaming Media Traffic**—audio-visual content that plays while downloading

To configure Application Filters settings:

1. Click **Detections** on the main menu. A drop-down menu displays.
2. Click **Application Filters** from the drop-down menu. The Application Filters screen displays.
3. Enable detection for **Instant Messaging**.

FIGURE 4-5. Instant Messaging options in Application Filters



a. Select the **Instant Messaging** check box.

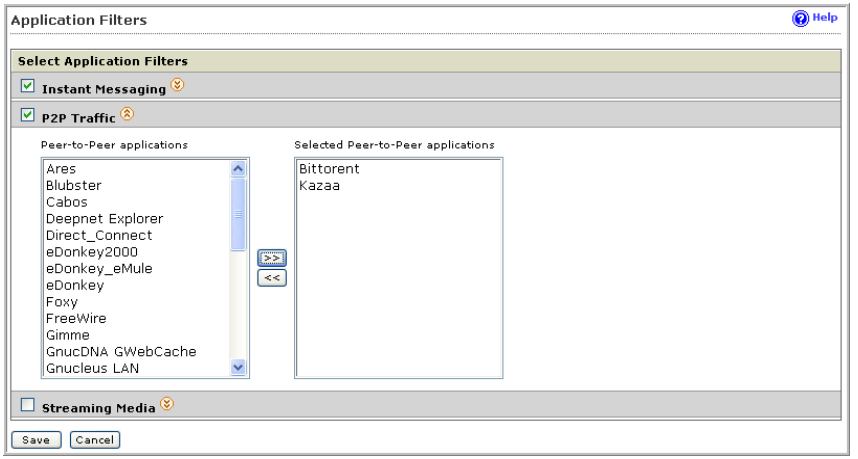
b. Select the specific protocols for detection.

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

c. Move the selected protocol under **Selected Instant Messaging protocols**.

4. Enable detection for **P2P Traffic**.

FIGURE 4-6. P2P Traffic options in Application Filters



a. Select the **P2P Traffic** check box.

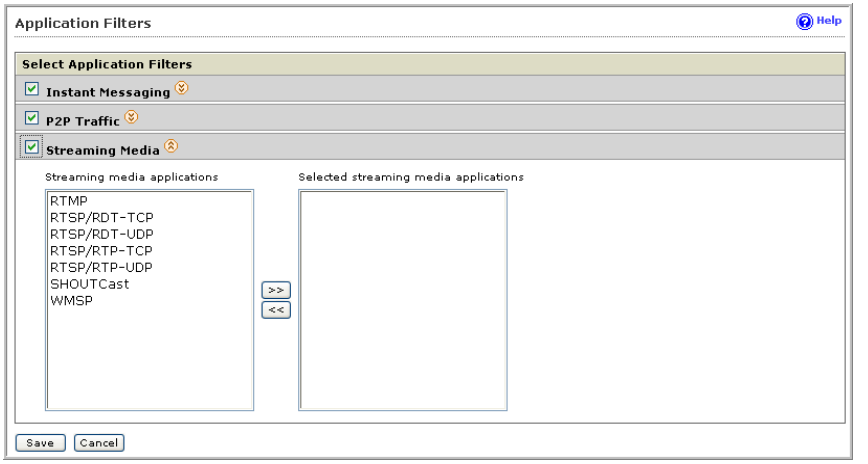
b. Select the specific protocols for detection.

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

c. Move the selected protocol under **Selected Peer-to-Peer applications**.

5. Enable detection for **Streaming Media**.

FIGURE 4-7. Streaming Media options in Application Filters



   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.

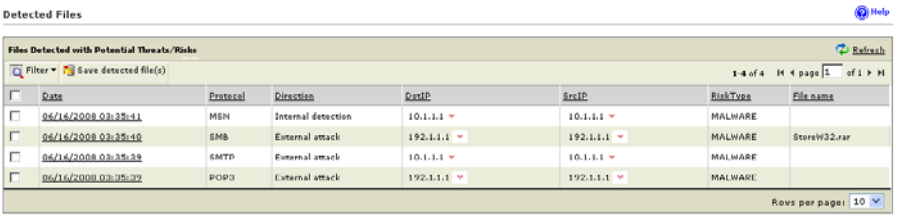
   c. Move the selected protocol under **Selected streaming media applications**.

6. Click **Save**.

Saving Detected Files

The Detected Files screen displays the files with potential security risks. A potential risk file is defined as a file detected as malicious by the Network Content Inspection Engine and Network Content Correlation Engine. Threat Discovery Appliance tags these files as potential security risks/threats and makes a copy of the files tagged as potential security risks/threats for assessment.

FIGURE 4-8. The Detected Files screen



The Detected Files screen displays the following information:

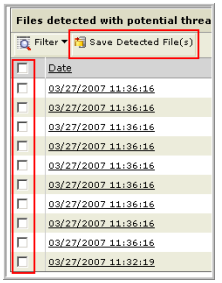
TABLE 4-1. Detected Files information

LOG INFORMATION	DESCRIPTION
Date	Date and time of the incident
Protocol	Protocols such as HTTP, FTP, SMTP, POP3, and others
Direction	Whether this is an internal detection or an external attack
DstIP	IP address of the client under attack
SrcIP	IP address of the source of the threat
RiskType	Detection type
File name	File name of the potential threat

Saving Multiple Files

The Detected Files screen can quickly save multiple suspicious files.

FIGURE 4-9. The Save Detected File(s) button



To save multiple detected files:

1. Click **Detections** on the main menu. A drop-down menu displays.
2. Click **Detected Files** from the drop-down menu. The Detected Files screen displays.

3. Select the files you want to save.
4. Click **Save detected file(s)**. Threat Discovery Appliance prompts you to save or open the compressed file format.
5. Click **Open** or **Save**.

Configuring the Detection Exclusion List

Exclude specific protocols and IP address ranges from the logs or from the Outbreak Containment Services block action.

Additionally, you can export and then import the network configuration file to another Threat Discovery Appliance device.

Adding Potential Threat Detections Exclusions

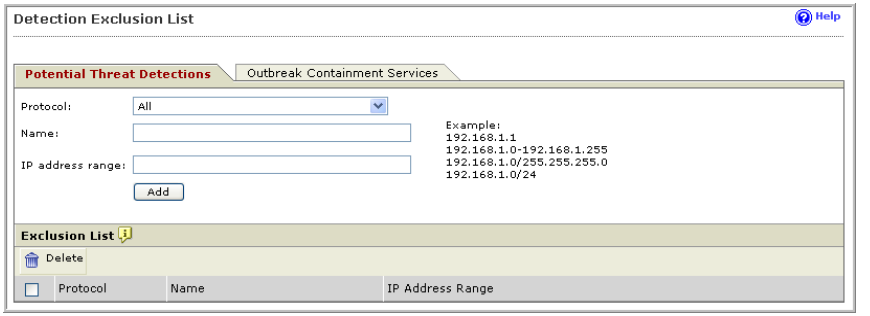
Exclude specific protocols and IP address ranges from the logs. Threat Discovery Appliance scans these IP addresses but potential threat detections will not appear in the logs.

Note: This list only excludes potential threat detections. Any known threat or application filter detections still appear in the logs.

To add to the exclusion list:

1. Click **Detections** on the main menu. A drop-down menu displays.
2. Click **Detection Exclusion List** from the drop-down menu. The Detection Exclusion List screen displays.

FIGURE 4-10. Potential Threat Detections tab in Detection Exclusion List screen



3. Select the **Potential Threat Detections** tab.
4. Select a **Protocol** from the drop-down list.
5. Specify a unique name for easy identification.
6. 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
7. Click **Add**.

Removing Potential Threat Detections Exclusions

Remove or delete IP addresses from the exclusion list.

To remove from the list:

1. Click **Detections** on the main menu. A drop-down menu displays.
2. Click **Detection Exclusion List** from the drop-down menu. The Detection Exclusion List screen displays.

3. Select the **Potential Threat Detections** tab.
4. Select the entry or entries you want to remove.
5. Click **Delete**.

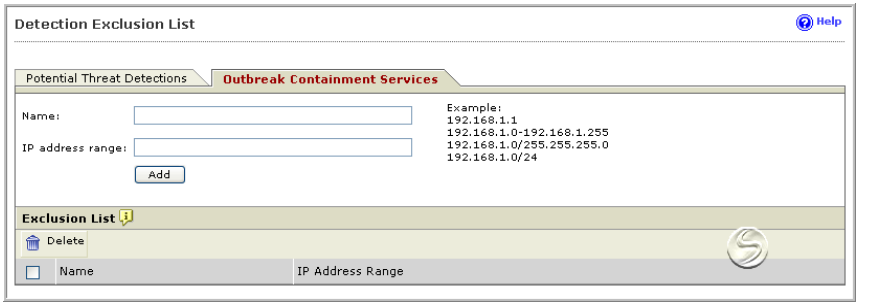
Adding Outbreak Containment Services Exclusions

Exclude IP address ranges from the Outbreak Containment Services block action. Include only trusted IP addresses to this list or an outbreak may occur.

To add to the exclusion list:

1. Click **Detections** on the main menu. A drop-down menu displays.
2. Click **Detection Exclusion List** from the drop-down menu. The Detection Exclusion List screen displays.

FIGURE 4-11. Outbreak Containment Services tab in Detection Exclusion List screen



3. Select the **Outbreak Containment Services** tab.
4. Specify a unique name for easy identification.
5. 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
6. Click **Add**.

Removing Outbreak Containment Services Exclusions

Remove or delete IP addresses from the exclusion list.

To remove from the list:

1. Click **Detections** on the main menu. A drop-down menu displays.
2. Click **Detection Exclusion List** from the drop-down menu. The Detection Exclusion List screen displays.
3. Select the **Outbreak Containment Services** tab.
4. Select the entry or entries you want to remove.
5. Click **Delete**.

Threshold Settings

Threat Discovery Appliance detects incidents that Trend Micro considers a possible threat.

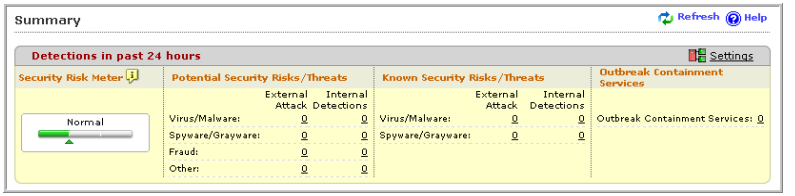
Configure the following statuses:

- **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 but does not necessarily mean an action needs to be done. This can be any value you set. Threat Discovery Appliance considers anything lower than this value as normal network behavior.

To configure the threshold settings:

1. Click **Summary** on the main menu.
2. Click **Settings** in Security Risk Meter. The Threshold Settings screen displays.

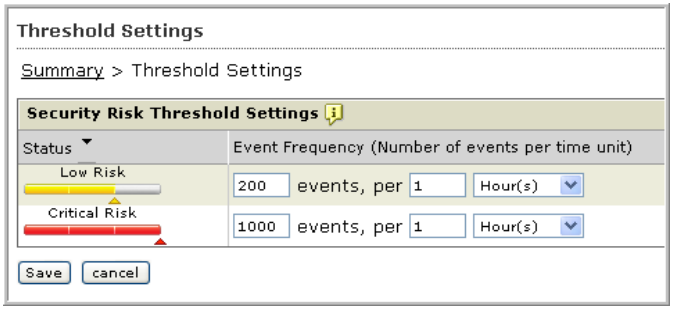
FIGURE 4-12. Detections in past 24 hours summary screen



3. In the **Low risk** setting, select the minimum number of events per time unit considered a low risk. For example, set 3 events per 1 hour as the Low risk threshold.

Note: The default value for Low Risk is 20 events for every minute. Trend Micro recommends adjusting this value according to the size of your network.

FIGURE 4-13. Threshold Settings screen



4. In the **Critical risk** setting, select the minimum number of events for every time unit considered a critical risk. For example, set 5 events per 1 hour as the Critical risk threshold.

Note: The default value for Critical Risk is 100 events for every minute. Trend Micro recommends adjusting this value according to the size of your network.

5. Click **Save**.

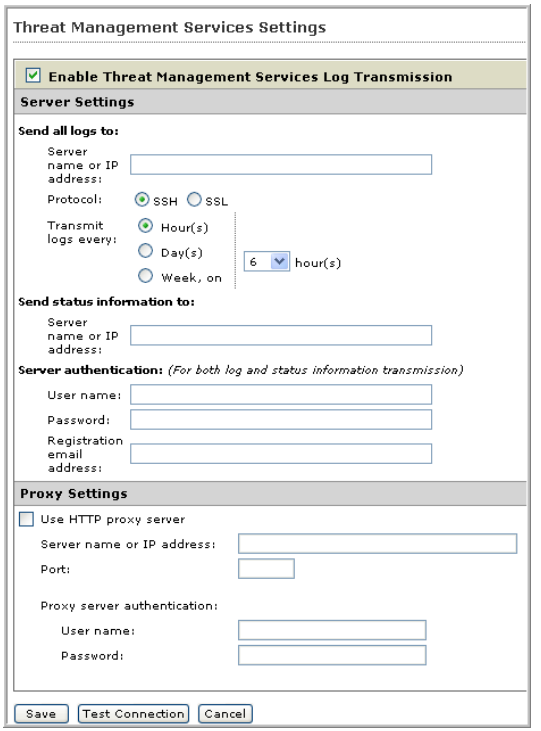
Configuring Threat Management Services Settings

The Trend Micro Threat Management Services Portal is a complete Software as a Service (SaaS) security portal that provides security solutions to small, medium, and enterprise businesses.

If you registered to use Threat Management Services, configure Threat Discovery Appliance to automatically send the logs to Threat Management Services. You can then view regular threat analysis reports from the portal.

This report contains security incidents and network activities logged by either the device or the policies you set. This report also contains Trend Micro recommended actions to prevent or address these incidents.

FIGURE 4-14. Threat Management Services screen



To configure Threat Management Services settings:

1. Click **Threat Management Services** on the main menu. The Threat Management Services Settings screen displays.
2. Select the **Enable Threat Management Services Log Transmission** option.

> **Note:** Configure the firewall to allow Port 443 traffic from Threat Discovery Appliance to Threat Management Services Portal.

3. Type the server name or IP address of the server where you send the logs.
4. Select the protocol. You can select either **SSH** or **SSL**.

Note: If selecting SSH, configure firewall to allow Port 22 traffic from Threat Discovery Appliance to Threat Management Services Portal.

5. Select the frequency of log transmissions.
6. Type the Server name or IP address of the server where you send the status information to.
7. Type the user name and password you use to log on to the Threat Management Services portal.
8. Type the email address you used to register to the Threat Management Services portal.
9. Configure the proxy settings.
   a. Select the **Use HTTP proxy server** option.
   b. Type the server name or IP address and the port number. For example, 192.1.1.1 and 1234 as the port number.
   c. If your proxy server requires authentication, type the user name and password under Proxy server authentication.
10. Click **Save**.

Configuring LeakProof™ Settings

LeakProof™ enables companies to reduce the risk of data breaches and ensures privacy and compliance. It also understands the content of data at rest, in use, or in motion on every enterprise endpoint, providing protection of sensitive data.

Trend Micro offers LeakProof as an enterprise class solution for preventing information leakage. LeakProof is a comprehensive solution which includes the detection of sensitive content like passwords and credit card numbers defined by administrators or users.

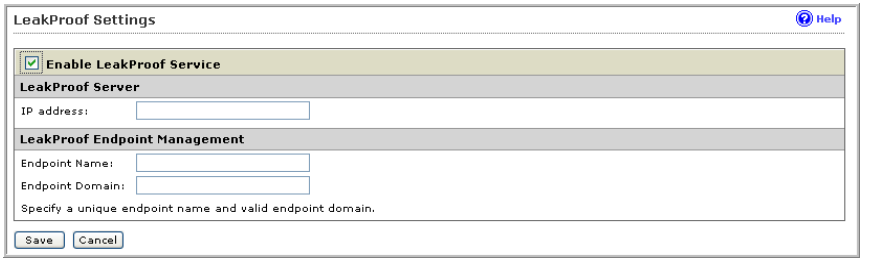
This product allows you to:

- Protect customer privacy and/or intellectual property
- Secure laptops and desktops
- Meet compliance-driven information technology initiatives

To configure LeakProof settings:

1. Click **LeakProof** on the main menu. The LeakProof Setting screen displays.

   FIGURE 4-15. LeakProof Settings screen



2. (Optional) Select **Enable/Disable LeakProof service**.

Note: You can register the LeakProof server without enabling the LeakProof service.

3. Type the IP address of the LeakProof Server device in the **IP address** field beside LeakProof Server.
4. Type the **Endpoint Name** and **Endpoint Domain**.
5. Click **Save**.

Product Integration

Threat Discovery Appliance is a stand-alone product. However, you can configure the device to work with Trend Micro products such as Trend Micro Control Manager™ and other mitigation devices such as Trend Micro™ Network VirusWall™ Enforcer to take advantage of the Threat Management Solution network analysis capabilities.

Registering to Mitigation Devices

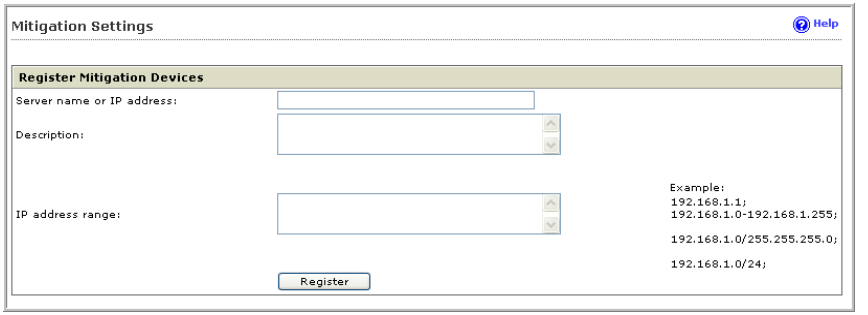
Register Threat Discovery Appliance to mitigation devices to make full use of the integration between these two products (See *Integration with Mitigation Servers* on page 6).

Note: You can register Threat Discovery Appliance to 20 mitigation devices.

To register Threat Discovery Appliance:

1. Click **Mitigation** on the main menu. A drop-down menu displays.
2. Click **Mitigation Settings** from the drop-down menu. The Mitigation Settings screen displays.

FIGURE 4-16. The Mitigation Settings screen

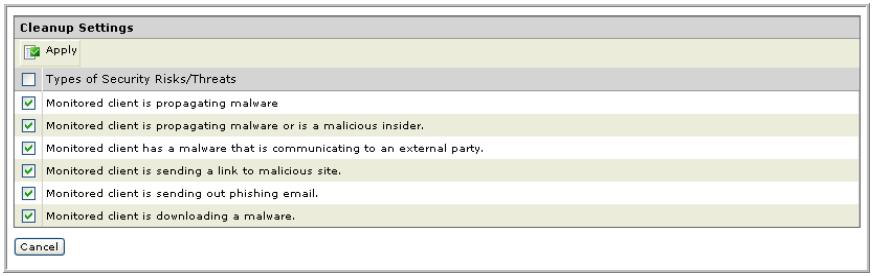


3. Under **Mitigation Settings**, type the mitigation device **Server name or IP address**.
4. Type a **Description** for the device.
5. Specify **IP address ranges**.

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

6. Click **Register**. The Cleanup Settings screen appears.

FIGURE 4-17. The Mitigation Settings option



7. Select the types of security risks/threats to send to the mitigation device.
8. Click **Apply**.

Registering to Control Manager

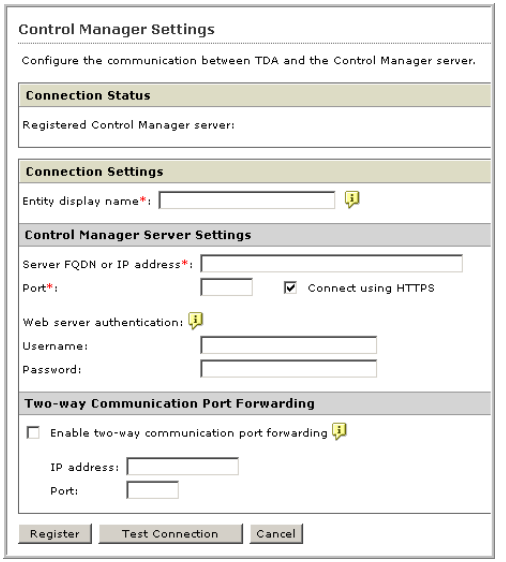
Register Threat Discovery Appliance to Control Manager to centrally manage the logs and data.

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

To register to Control Manager:

1. Click **Administration** on the main menu. A drop-down menu appears.
2. Click **Control Manager Settings**. The Control Manager Settings screen displays.

FIGURE 4-18. The Control Manager Settings screen



3. Under **Connection Settings**, type the name of the Threat Discovery Appliance device in the Entity display name field.

> **Note:** Select this name carefully because this is the name that displays in the Control Manager server Product Directory that identifies the Threat Discovery Appliance device. A unique and meaningful name will help you quickly identify the Threat Discovery Appliance device in the Control Manager Product Directory.

4. Under **Control Manager Server Settings**:
   a. Type the Control Manager server IP address or host name in the Server FQDN or IP address field.

b. Type the port number that the MCP agent uses to communicate with Control Manager.

Note: Management Communication Protocol (MCP) is Trend Micro's next generation agent for managed products. MCP is the way Control Manager communicates with Threat Discovery Appliance devices.

c. If you have Control Manager security 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 any managed products), select **Connect through HTTPS**.

d. If your network requires authentication, type the user name and password for your IIS server in the Username and Password fields.

5. 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.

Refer to the *Trend Micro Control Manager Administrator's Guide* for more information about managing products in Control Manager 5.0.

Backup/Restore

You can export configuration data for backup purposes or to deploy the configuration data to another Threat Discovery Appliance device.

You can also import the configuration file from a backup file or from another device to quickly replicate configuration settings.

Note: Trend Micro recommends regularly backing up the Threat Discovery Appliance settings.

Backing Up Device Configuration Settings

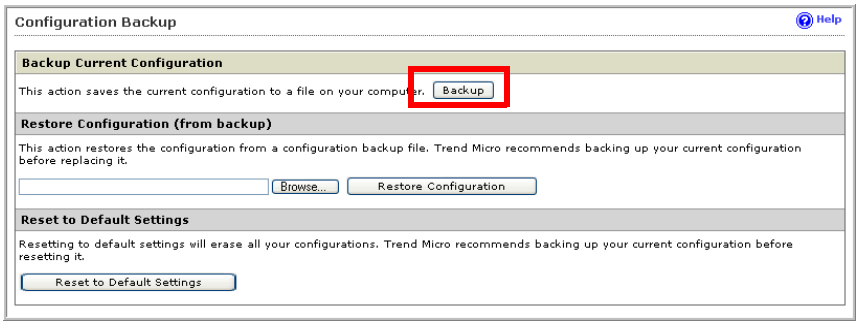
Backing up device configuration settings stores both the network and device configurations to an encrypted file. Making backup copies of your device configuration settings ensures you can restore your settings in case of a problem, or replicate them to another device.

Note: Configuration settings are encrypted and cannot be modified.

To back up the configuration file:

1. Click **Administration** on the main menu. A drop-down menu displays.
2. Click **Backup/Restore** from the drop-down menu. The Configuration Backup screen displays.

FIGURE 4-19. Configuration Backup screen



3. Click **Backup** under **Backup Current Configuration**. A File Download screen displays.
4. Select **Save** and specify the location to which the configuration file saves.
5. Click **Save**.

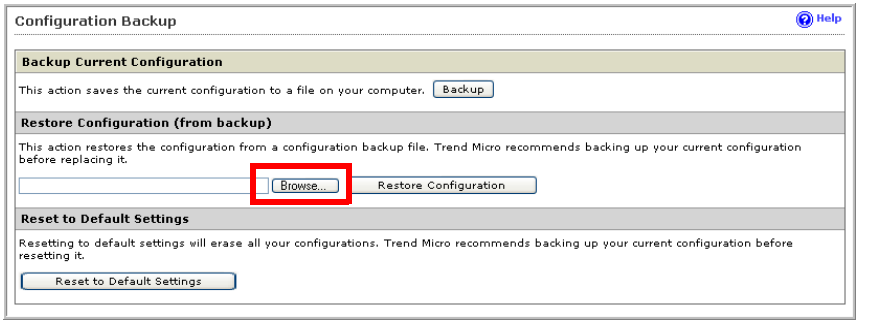
Restoring Device Configuration Settings

You can restore the configuration from a backup file or from another device. Importing a configuration file overwrites all current settings. Back up the current configuration settings before importing the configuration file.

To restore the configuration file:

1. Click **Administration** on the main menu. A drop-down menu displays.
2. Click **Backup/Restore** from the drop-down menu. The Configuration Backup screen displays.

FIGURE 4-20. Configuration Backup screen



3. Click **Browse** under **Restore Configuration (from backup)**. The Choose File screen appears.
4. Select the file to import and click **Restore Configuration**. The confirmation message appears.
5. Click **OK**. Threat Discovery Appliance restarts after importing the configuration file.
6. Configure the IP address settings (see *Configuring IP Address Settings* on page 3-4).

Resetting Device Settings

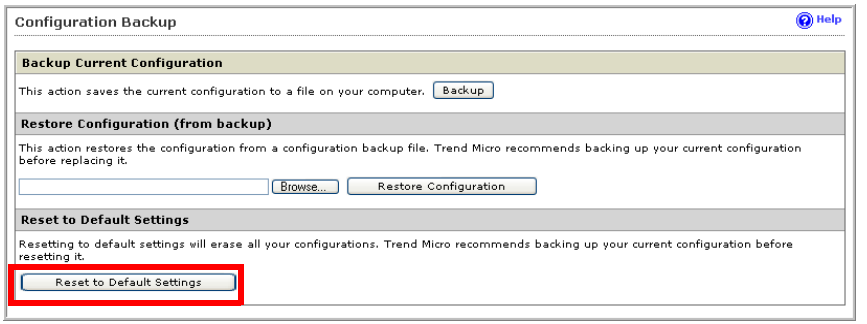
Resetting the device reverts Threat Discovery Appliance to default settings.

WARNING! Resetting to the default settings overwrites all current settings. Back up the current configuration file before resetting to the default device settings.

To restore the default settings:

1. Click **Administration** on the main menu. A drop-down menu displays.
2. Click **Backup/Restore** from the drop-down menu. The Configuration Backup screen displays.

FIGURE 4-21. Configuration Backup screen



3. Click **Reset to Default Settings** under **Reset Default Settings.** The confirmation message appears.
4. Click **OK**.

Updating the Firmware

Use this screen to update the Threat Discovery Appliance firmware. Restart the device and then migrate the configuration files to finish the update.

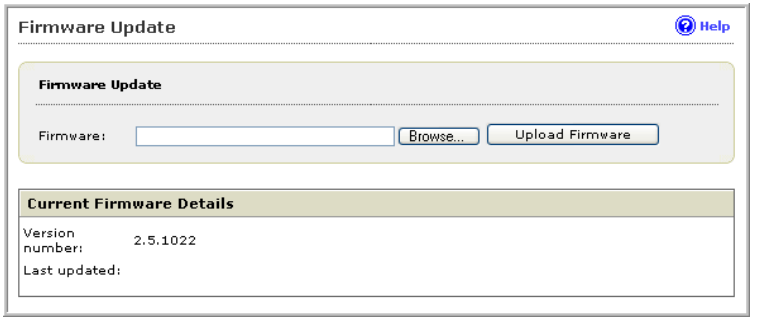
Note: Check the current Threat Discovery Appliance firmware details and verify the software version to ensure you want to proceed with the update.

To update the firmware:

1. Download the Threat Discovery Appliance firmware image from the Trend Micro Web site or from your Trend Micro reseller.
2. Extract the file to any folder on your computer.

3. Click **Administration** on the product console main menu. A drop-down menu displays.
4. Click **Firmware Update** from the drop-down menu. The Firmware Update screen appears.

FIGURE 4-22. Firmware Update screen



5. Click **Browse** and go to the folder where you extracted the firmware image.

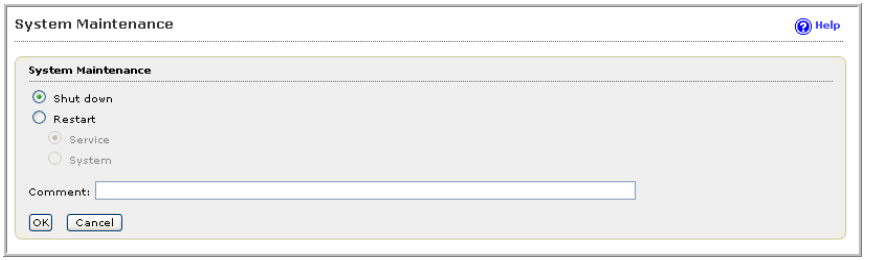
WARNING! **Back up the configuration settings (See *Backing Up Device Configuration Settings* on page 28) before updating the Threat Discovery Appliance firmware.**

6. Click **Upload Firmware**. The Migration configuration option appears. If you enable this option, you will retain your current settings. Otherwise, the update will revert your configuration to the default settings.
7. Click **Continue**. Wait for a couple of minutes as the device restarts. The Log on screen appears after the device finishes the update.
8. Configure the proxy settings and registerto Control Manager again.

System Maintenance

Shut down or restart the Threat Discovery Appliance device, system, or service from the **System Maintenance** screen on the product console.

FIGURE 4-23. The System Maintenance screen



Shutting Down Threat Discovery Appliance

Shut down the device from the **System Maintenance** screen on the product console.

To shut down the device:

1. Click **Administration** on the main menu. A drop-down menu displays.
2. Click **System Maintenance** from the drop-down menu. The System Maintenance screen displays.
3. Select **Shut down** under System Maintenance.
4. (Optional) Specify a reason for shutting down the device beside **Comment**.
5. Click **Ok**.

Restarting Threat Discovery Appliance Services

Restart the Threat Discovery Appliance services from the **System Maintenance** screen on the product console.

To restart the services:

1. Click **Administration** on the main menu. A drop-down menu displays.
2. Click **System Maintenance** from the drop-down menu. The System Maintenance screen displays.
3. Select **Restart > Services** under System Maintenance.
4. (Optional) Specify a reason for restarting the services beside **Comment**.
5. Click **Ok**.

Restarting Threat Discovery Appliance

Restart the Threat Discovery Appliance device from the **System Maintenance** screen on the product console.

To restart the device:

1. Click **Administration** on the main menu. A drop-down menu displays.
2. Click **System Maintenance** from the drop-down menu. The System Maintenance screen displays.
3. Select **Restart > System** under System Maintenance.
4. (Optional) Specify a reason for restarting the device beside **Comment**.
5. Click **Ok**.

Chapter 5

Viewing and Analyzing Information

This chapter includes information about identifying security risks and evaluating Trend Micro™ Threat Discovery Appliance virus/malware protection practices.

The topics discussed in this chapter are:

- *Status Indicators* on page 5-2
- *Status Indicators* on page 5-2
- *Using Notifications* on page 5-8
- *Viewing Logs and Reports* on page 5-18
- *Logs* on page 5-24

Status Indicators

Trend Micro™ Threat Discovery Appliance displays status indicators from the upper left-hand corner of the main menu.

FIGURE 5-1. Status Indicators

Risk Meter

Risk Meter displays the security risk status of the network that Threat Discovery Appliance monitors. Configure these settings in the Threshold Settings screen. 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 but no actions needs to be performed.
- **Critical risk**—a red indicator signifies that there is a need to constantly monitor the network and take preventive or corrective action.

Appliance Health

Appliance Health displays the temperature and fan speed status of the Threat Discovery Appliance device.

- **Normal**—a green indicator signifies that the device temperature is normal.
- **Warning**—a yellow indicator signifies that the device or CPU temperature is between 90-100% of the limit. Check the device temperature or ensure that the fan is working.

- **Critical**—a red indicator signifies that the device or CPU temperature is 100% or higher than the safe range. Check the device temperature or ensure that the fan is working.

Network Flow

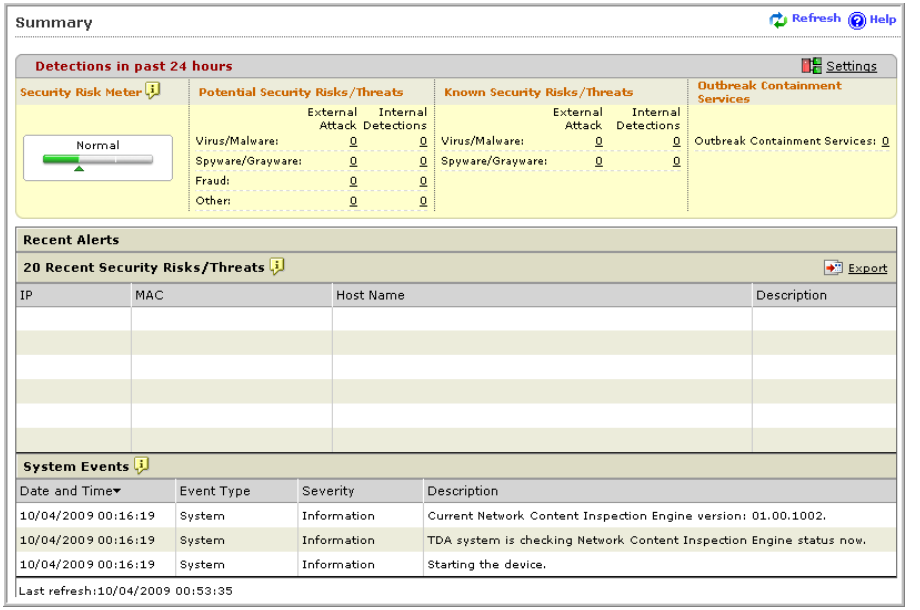
Network flow displays the current status of the network Threat Discovery Appliance scans. The network flow status indicates the following:

- **Normal**—a green indicator signifies that Threat Discovery Appliance handles the traffic flowing through the network and device.
- **Critical**—a red indicator signifies that the network flow exceeds Threat Discovery Appliance device capacity. Verify the capacity of the switch mirror port and the network traffic.

Viewing the Summary Screen

When you open the product console or click **Summary** on the main menu, the Summary screen appears as shown in *Figure 5-2*.

FIGURE 5-2. The Summary screen

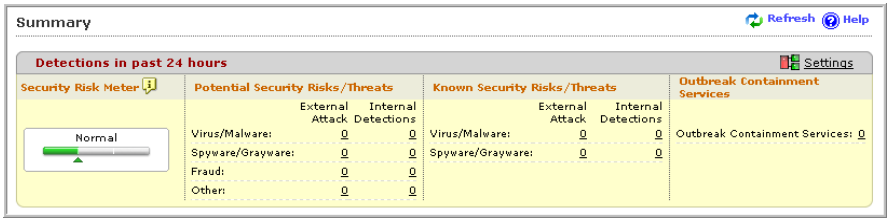


Note: The Summary screen automatically resets every 10 seconds. Click **Refresh** to display the latest information on this screen.

Detections in Past 24 Hours

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

FIGURE 5-3. Detections in past 24 hours



Security Risk Meter

Security Risk Meter shows the degree of security risk according to the incidents Threat Discovery Appliance detected over the past 24 hours. The degree or risk is dependent on the threshold settings you configure (see *Threshold Settings* on page 4-18).

Potential Security Risks/Threats

Potential Security Risks/Threats shows the number of potential security risks/threats the device detected over the past 24 hours. This means certain actions or events alerted Threat Discovery Appliance of a possible security risk/threat. This is applicable for attacks coming from outside the network and attacks coming from inside the network.

Note: Click the number of detections for more details on the incident.

Known Security Risks/Threats

Known Security Risks/Threats shows the number of known security risks/threats that try to enter the network or are already inside the network.

Note: Click the number of detections for more details on the incident.

Outbreak Containment Services

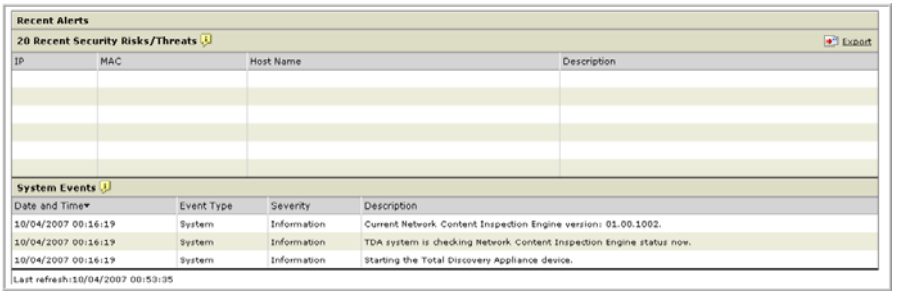
Outbreak Containment Services shows the current number of potential malware activities Threat Discovery Appliance detected that might cause an outbreak.

Note: Click the number of events for additional information.

Recent Alerts

Displays the summary of events that recently occurred. This includes the 20 most recent security risks/threats and system events.

FIGURE 5-4. Recent Alerts summary



20 Recent Security Risks/Threats

The 20 recent security risks/threats display the most recent known threats and potential threats that have "High" severity rating.

The logs display the IP address, MAC address, Host name, and description of the security risks/threats. To reduce the number of duplicate logs, Trend Micro groups the logs with the same IP address, MAC address, and description. Click the event or threat to display detailed information for one or more logs.

Note: Click the **Export** button to export additional security risks/threats details to a .csv file.

A virus or malware name under **Descriptions** indicates a known threat. A rule or policy name specified by the Network Content Correlation Engine or Pattern indicates a Potential threat.

Note: Contents in this alert are not limited to the past 24 hours.

System Events

The system events show device information and component or device update events. This means that whenever the device restarts, or encounters device problems, Threat Discovery Appliance logs these events.

Using Notifications

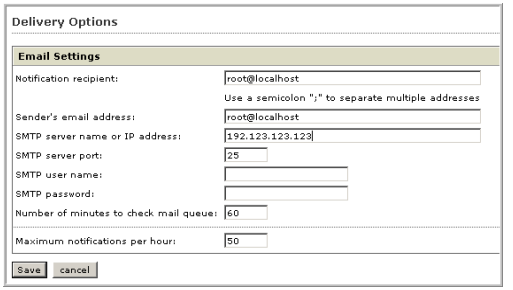
Threat Discovery Appliance can send notifications to designated individuals when specific events occur, even if you are not monitoring the network. Notifications help determine the action(s) required in the event of an outbreak.

Configure the notifications you want to receive and the notification sender and recipients in the following Notification screens.

Configuring Delivery Options

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.

FIGURE 5-5. The Delivery Options screen



To configure the delivery options:

1. Click **Notifications** on the main menu. A drop-down menu displays.
2. Click **Delivery Options** from the drop-down menu. The Delivery Options screen displays.
3. Under **Notification recipient**, type the default recipient.

> **Note:** Use a semicolon ";" to separate multiple addresses.

4. Under **Sender's email address**, type the default sender.

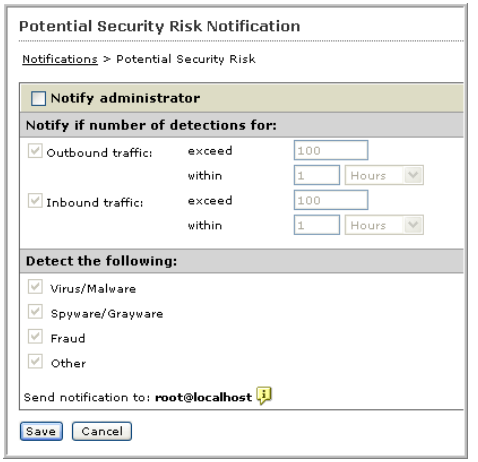
Note: You can only add one valid email address.

5. Under **SMTP server name or IP address**, type the SMTP server name or IP address.
6. Under **SMTP server port**, type the SMTP server port.
7. Specify the SMTP user name and password. Ensure that you add the Threat Discovery Appliance IP address to the SMTP relay list and host name to the DNS server to ensure you receive the notifications.
8. Specify the maximum number of notifications and the number of minutes to check the mail queue. Trend Micro recommends using the default settings.
9. Click **Save**.

Configuring Potential Security Risk Notifications

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. These notifications can help prevent or contain network outbreaks caused by unknown Internet security risks/threats.

FIGURE 5-6. The Potential Security Risk screen



To configure notifications for detection of potential security risks:

1. Click **Notifications** on the main menu. A drop-down menu displays.
2. Click **Notification Settings** from the drop-down menu. The Notification Settings screen displays.
3. Under **Configure Notifications for Following Events**, click the **Detection of potential security risks** link. The Potential Security Risk Notification screen displays.
4. Select the **Notify administrator** option.
5. 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 within the network
   - **Inbound traffic** means detections coming from outside the network

6. 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.

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

Disabling Potential Security Risk Notifications

Disable the potential security risk notifications only if you do not want to be informed of security risks.

To disable notifications:

1. Click **Notifications** on the main menu. A drop-down menu displays.
2. Click **Notification Settings** from the drop-down menu. The Notification Settings screen displays.
3. Under **Configure Notifications for Following Events**, click **Detection of potential security risks**. The Potential Security Risk Notification screen displays.
4. Clear the **Notify administrator** option.
5. Click **Save**.

Configuring Known Security Risk Notifications

Threat Discovery Appliance can send an email when it detects known security risks. These are security risks/threats that can come from the internal network or from an external attack. Use the Known Security Risk Notifications screen to configure the notifications sent to the designated individuals.

FIGURE 5-7. The Known Security Risk screen

To configure notifications for detection of known security risks:

1. Click **Notifications** on the main menu. A drop-down menu displays.
2. Click **Notification Settings** from the drop-down menu. The Notification Settings screen displays.
3. Under **Configure Notifications for Following Events**, click the **Detection of known security risks** link. The Known Security Risk Notification screen displays.
4. Select the **Notify administrator** option.
5. 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 within the network
   - **Inbound traffic** means detections coming from outside the network
6. 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.

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

Disabling Known Security Risk Notifications

Disable the known security risk notifications only if you do not want to be informed of security risks.

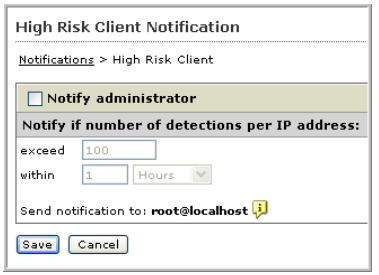
To disable notifications:

1. Click **Notifications** on the main menu. A drop-down menu displays.
2. Click **Notification Settings** from the drop-down menu. The Notification Settings screen displays.
3. Under **Configure Notifications for Following Events**, click **Detection of known security risks**. The Known Security Risk Notification screen displays.
4. Clear the **Notify administrator** option.
5. Click **Save**.

Configuring High Risk Client Notification

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 the client has many detections and resolve this issue before it becomes the source of an outbreak.

FIGURE 5-8. The High Risk Client screen



To configure notifications for detection of high risk clients:

1. Click **Notifications** on the main menu. A drop-down menu displays.
2. Click **Notification Settings** from the drop-down menu. The Notification Settings screen displays.
3. Under **Configure Notifications for Following Events**, click **Detection of high risk clients**. The High Risk Client Notification screen displays.
4. Select the **Notify administrator** option.
5. Under **Notify if number of detections per IP address**, configure the number of detections per IP address that triggers an alert.
6. 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.

7. Click **Save**.

Disabling High Risk Client Notifications

Disable the high risk client notifications only if you do not want to be informed of high risk clients.

To disable notifications:

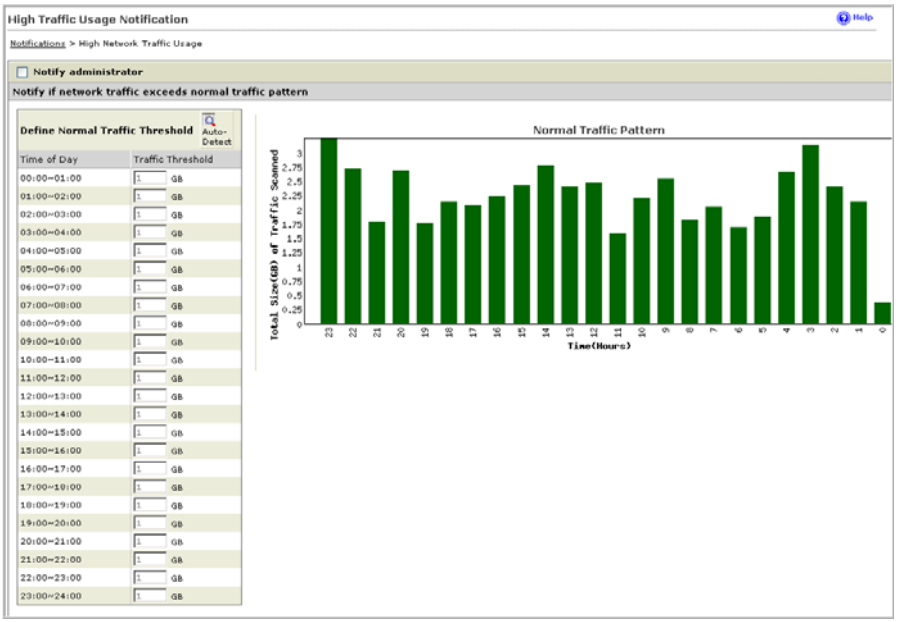
1. Click **Notifications** on the main menu. A drop-down menu displays.
2. Click **Notification Settings** from the drop-down menu. The Notification Settings screen displays.
3. Under **Configure Notifications for Following Events**, click **Detection of high risk clients**. The High Risk Client Notification screen displays.
4. Clear the **Notify administrator** option.
5. Click **Save**.

Configuring High Network Traffic Usage Notifications

Threat Discovery Appliance can send an email when network traffic usage exceeds a certain threshold. There are times when this happens because of an external attack. Use the High Traffic Usage Notification screen to configure notifications sent to designated individuals.

Note: The data for these tables resets if the device restarts or shuts down.

FIGURE 5-9. The High Traffic Usage screen



Note: The numbers 0-23 Time (Hours) at the lower part of the Normal Traffic Pattern graph shows the time that passed since Threat Discovery Appliance scanned and produced the graph. However, this does not signify the time Threat Discovery Appliance scanned the network. For example, the ones in 0 Time (Hours) shows the current traffic value while those in number 4 Time (Hours) occurred 4 hours before.

To configure notifications for detection of high network traffic usage:

1. Click **Notifications** on the main menu. A drop-down menu displays.
2. Click **Notification Settings** from the drop-down menu. The Notification Settings screen displays.
3. Under **Configure Notifications for Following Events**, click **High network traffic usage**. The High Traffic Usage Notification screen displays.
4. Select the **Notify administrator** option.

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

Disabling High Network Traffic Usage Notifications

Disable the high network traffic usage notification only if you do not want to be informed of network usage.

To disable notifications:

1. Click **Notifications** on the main menu. A drop-down menu displays.
2. Click **Notification Settings** from the drop-down menu. The Notification Settings screen displays.
3. Under **Configure Notifications for Following Events**, click **High network traffic usage**. The High Traffic Usage Notification screen displays.
4. Clear the **Notify administrator** option.
5. Click **Save**.

Viewing Logs and Reports

Use logs to monitor Threat Discovery Appliance and how it scans and determines incidents in your network. *Table 5-1* explains the types of logs and reports available in Threat Discovery Appliance.

TABLE 5-1. Log types

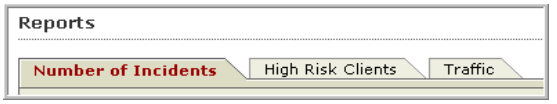
TYPE	DESCRIPTION
Detection logs	Information on potential and known threats, external attacks, and internal detections. This includes viruses, Trojans, and spyware. To view the virus log, select **Logs > Detection Log Query.**
Application Filter logs	Information on the application filter activities inside or outside the network.
System logs	Summaries of events regarding the device or the device, such as component updates and device restarts. To view the program log, select **Logs > System Log Query**.

Reports

The Threat Discovery Appliance report provides an online collection of figures about incidents or detections, clients, and the traffic that occurs in the network. These reports display in a variety of formats, including tables, bar, line, and pie graphs. These reports are shown in 3 tabs:

- Number of Incidents
- High Risk Clients
- Traffic

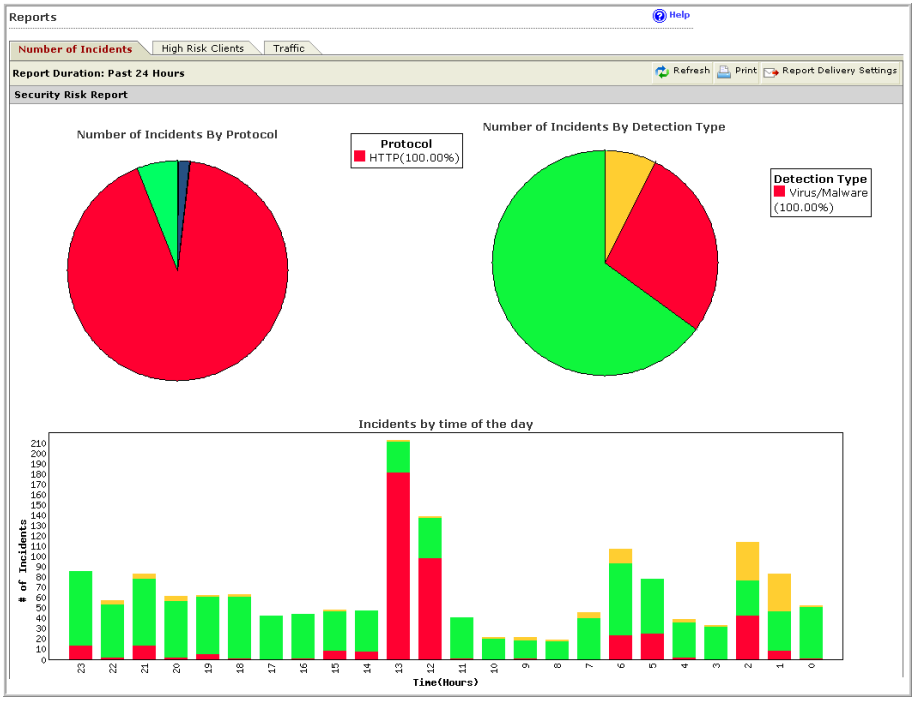
FIGURE 5-10. The Reports screen tabs



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 5-11. Number of Incidents report



Number of Incidents by Protocol

The **Number of Incidents by Protocol** displays the protocols 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 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

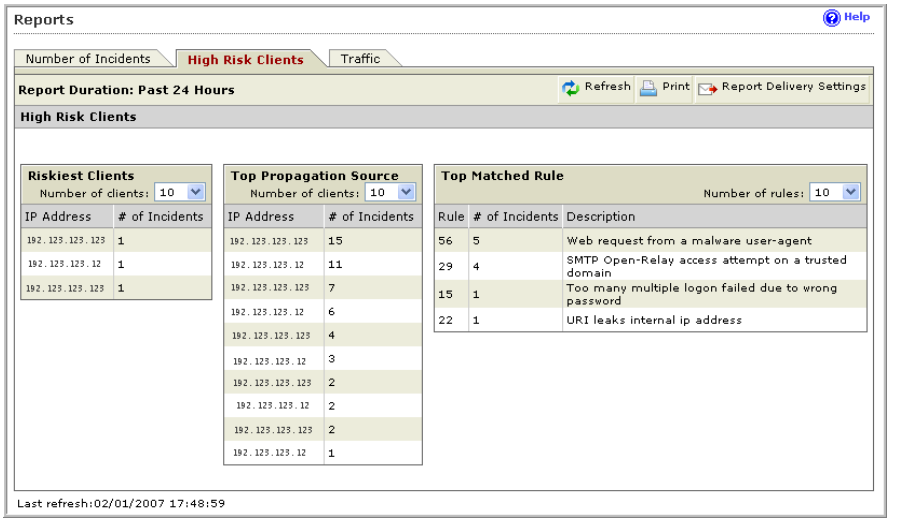
The numbers 0-23 Time (Hours) at the lower part of the graphs show the time that passed since Threat Discovery Appliance scanned and produced the graph. However, this does not signify the time Threat Discovery Appliance scanned the network. For example, the ones in 0 Time (Hours) show the current traffic value while those in number 4 Time (Hours) occurred 4 hours before.

High Risk Clients

The High Risk Client tab displays daily reports of the riskiest clients, top propagation source, and top matched rule. Both the Riskiest Clients and Top Propagation Source tables show the IP address and number of incidents. The Top Matched Rule table shows the triggered rules, the number of incidents, and rule descriptions.

Note: The triggered rules in the Top Matched Rule table are rules that Trend Micro established using the Network Content Inspection Engine and Network Content Correlation Engine. Trend Micro continuously updates the Network Content Inspection Engine and Network Content Correlation Engine pattern and rules.

FIGURE 5-12. High Risk Clients report



Traffic

The Traffic tab displays the daily traffic scanned per hour of the day, traffic scanned per protocol, and file types that go through the network. This includes tables pertaining to the HTTP, SMTP, and other protocols.

Note: The data for these tables resets if the device restarts or shuts down.

Traffic Scanned

The numbers 0-23 Time (Hours) at the lower part of the graphs indicate the time that passed. For example, the ones in 0 Time (Hours) show the current traffic value or 0 hours passed, while those in number 4 Time (Hours) occurred 4 hours before or 4 hours has passed.

Total Traffic Scanned

Displays the summary of network traffic scanned for the past 24 hours.

Traffic (in GB) Scanned per Protocol

Displays the network traffic scanned for the past 24 hours, separated by protocol, specifically, HTTP, SMTP, and other protocols.

FIGURE 5-13. Traffic report

Traffic by File Types (Number of Files)

Displays the types of files either sent or received from the network for the past 7 days.

Configuring Report Delivery Settings

Use the report delivery settings to receive daily reports on the security risk and/or traffic by email.

To receive daily reports:

1. Click **Report** on the main menu.
2. On the upper right hand corner of the screen, click the **Report Delivery Settings** button. The Report Delivery Settings screen displays.
3. Select the **Send email notifications everyday at 5:00 AM** option.
4. Click **Save**.

Disabling Report Delivery Notifications

Disable the report delivery notifications only if you do not want to receive regular reports.

To disable the reports:

1. Click **Report** on the main menu.
2. On the upper right hand corner of the screen, click the **Report Delivery Settings** button. The Report Delivery Settings screen displays.
3. Remove the **Send email notifications everyday at 5:00 AM** option.
4. Click **Save**.

Logs

Threat Discovery Appliance uses logs to save the information and activities that it detects in the network. You can use the Detection Log Query, Application Filter Log Query, or System Log Query to find information on network detections or appliance information, send logs to a Syslog Server, enable Threat Management Services, or maintain the size of the log database.

Viewing Detection Log

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.

You can also click the **Export** Logs button to immediately export the logs to a .CSV file or use the quick configuration link by mousing over an IP address and adding it to the network configurations.

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

To query the detection log database:

1. Click **Logs** on the main menu. A drop-down menu displays.
2. Click **Detection Log Query** from the drop-down menu. The Detection Log Query screen displays.
3. Select the **Protocol** type. Select more than one protocol by pressing SHIFT and the protocols or CTRL and the selected protocols.
4. Select the **Traffic** direction. Select from **Internal attacks**, **External detections**, or both.
5. 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.

6. Select **Mitigation** type of endpoint computers. Select from **Mitigated** and/or **Un-Mitigated**.

7. Select the **Severity** of the security risk. Select from **High**, **Medium**, **Low**, and/or **Informational** logs.
8. Select the **Group name**:
   - **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
9. Select the **Network Zone**. Select from **Trusted**, **Untrusted**, and/or **No network zone**.
10. Specify the **Date range** or click the calendar icon and select the date you want.
11. Select the IP address(es). Select from **All**, **IP address**, or a range of IP addresses.
12. (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.

---

13. Enable **Show executive logs** to view only high level logs.
14. Click **Display Logs**.

Note: The following steps are optional.

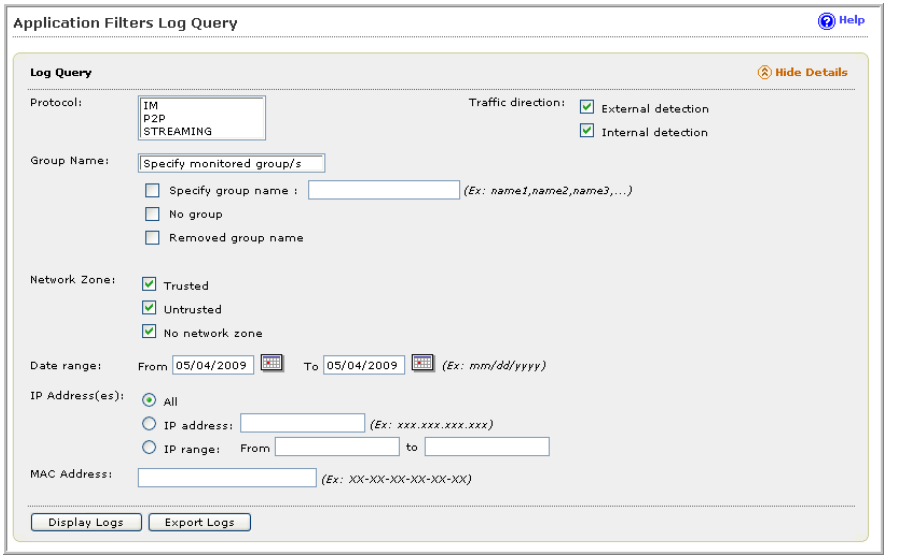
---

15. 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.
16. Click **Print** to print the logs or **Export** to export the file to a `.CSV` file format.

Viewing Application Filters Logs

Use this query to determine application filter activities inside or outside the network.

FIGURE 5-14. Application Filters Log Query screen



To query the application filters log query:

1. Click **Logs** on the main menu. A drop-down menu displays.
2. Click **Application Filter Log Query** from the drop-down menu. The Application Filter Log Query screen displays.
3. Select the protocol type. You can select **Instant Messaging**, **P2P**, or **Streaming Media Traffic**.
4. Select the traffic direction. You can select **Internal attacks**, **External detections**, or both.
5. Select the severity of the security risk. You can select from **High**, **Medium**, **Low**, or **Informational**.
6. Select the group name:
   - **Group name**—select from one of the group names in the list

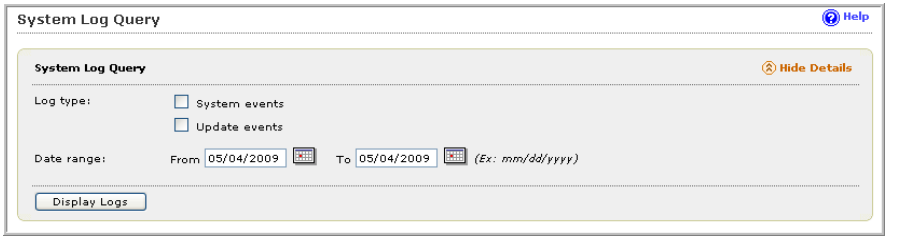
- **Specify group name**—type the specific group name the name including deleted group names
- **Removed group**—select this option if the group name is not available in the list and you cannot remember the exact name, for example, if the group name has been deleted
- **No group**—select this option for those that do not fall under any of the other categories

7. Select the network zone. You can 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 from the IP addresses options. You can select all the IP addresses, a certain IP address, or a range of IP addresses.
10. Click **Display Logs**.
11. Click **Print** to print the logs or **Export** to export the file to a `.CSV` file format.

Viewing System Logs

Use this query to determine the status of the device.

FIGURE 5-15. System Logs screen



To query the system log database:

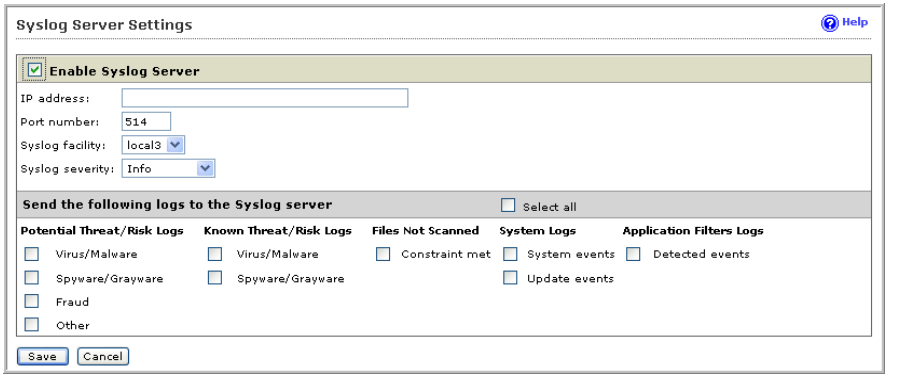
1. Click **Logs** on the main menu. A drop-down menu displays.
2. Click **System Log Query** from the drop-down menu. The System Log Query screen displays.
3. Select a log type. Select **System events**, **Update events**, or both.
4. Specify the date range or click the calendar icon and select the date you want.

5. Click **Display Logs**.

Configuring Syslog Server Settings

Some companies use Syslog servers to maintain and organize logs that come from different products.

FIGURE 5-16. Syslog Server Settings screen



To configure the Syslog servers settings:

1. Click **Logs** on the main menu. A drop-down menu displays.
2. Click **Syslog Server Settings** from the drop-down menu. The Syslog Server Settings screen displays.
3. Click the **Enable Syslog Server** option.
4. Type the IP address and port number of the Syslog server.
5. Select the syslog facility and severity.
6. Select the logs to send to the Syslog server.
7. Click **Save**.

Maintaining Logs

Use this screen to manually delete logs. Periodically check this screen to maintain the log database.

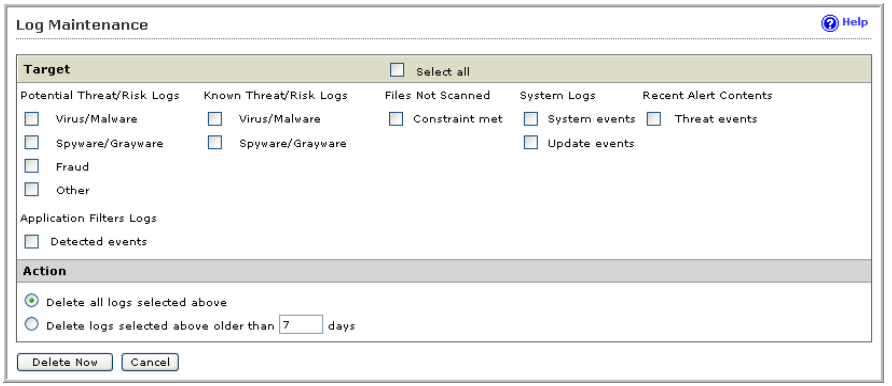
Threat Discovery Appliance maintains the logs in the device hard disk, in the Syslog server, or Trend Micro Control Manager.

Tip: Trend Micro recommends manually deleting logs regularly to keep the size of your logs from occupying too much space on your hard disk.

For example, you can manually delete all logs older than 7 days.

Note: Deletion of logs depends on your environment and the quantity of logs that you want to retain. However, if your logs reach 1,000,000 logs, the device automatically deletes 1% of the oldest logs.

FIGURE 5-17. Log Maintenance screen



To configure log settings:

1. Click **Logs** on the main menu. A drop-down menu displays.
2. Click **Log Maintenance** from the drop-down menu. The Log Maintenance screen displays.

3. Select the logs you want to delete. For example, you can select everything under Known Threats/Risk Logs and System Logs or you can **Select all** logs.
4. 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.
5. Click **Delete Now**.

Chapter 6

Preconfiguration and Rescue

This chapter explains how to configure basic Trend Micro™ Threat Discovery Appliance settings using the Preconfiguration console and how to rescue the device.

The topics discussed in this chapter are:

- *Using the Preconfiguration Console* on page 6-2
- *Rescuing Threat Discovery Appliance* on page 6-25

Using 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 device IP address and host name
- Restart the device
- View system logs

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

Entering the Preconfiguration Console

To access the Preconfiguration console:

1. Connect a computer to one of the following ports:
   - Management—use the Ethernet cable and connect it to the management port or connect the device to the switch. You must have an application that supports SSH communications, such as PuTTY.

     Note: Your computer's IP address must be in the same subnet as the Management port's IP address.

   - Console—use the RS232 serial cable and connect it to the port labeled **Console**. You must have an application that supports serial communications, such as HyperTerminal.

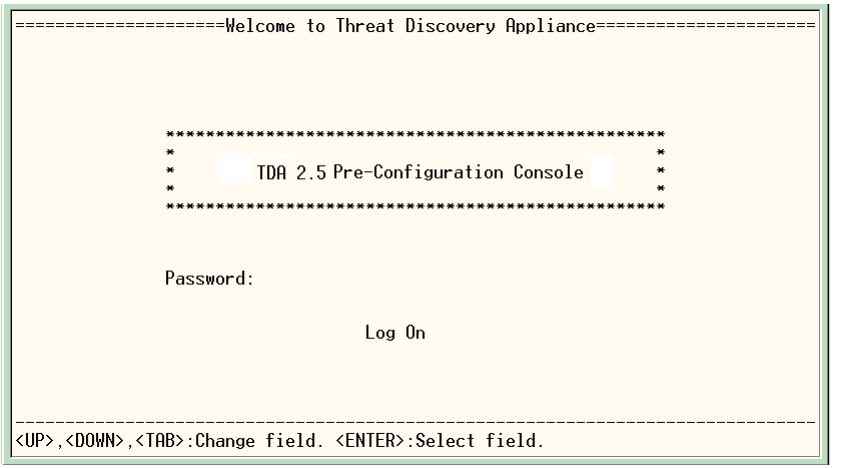
   To connect to Threat Discovery Appliance from another computer in your network (not directly connected to the device), ensure that you access the computer connected to the managed port.

   If you are accessing the managed port for the first time, do the following:

2. Configure the managed port network settings (see *Configuring Device Settings* on page 6-7).
3. Log on to a computer in your network.
   a. For an SSH connection, use the following values:
      - IP address (Managed port)—`192.168.252.1`
      - User name—tda
      - Password— [Just press Enter]
      - Port number —22
   b. For a HyperTerminal connection, use the following values:
      - Bits per second—115200
      - Data bits—8
      - Parity—None
      - Stop bits—1
      - Flow control—None
4. After setting up the connections, access the Preconfiguration console from the console port
5. Access the Preconfiguration console. The default password is **admin**.

WARNING! **Change the password immediately after logging on (See *Changing the Product Console Password* on page 4).**

FIGURE 6-1. The Log On screen



Preconfiguration Console Overview

The Preconfiguration console menu displays the following:

FIGURE 6-2. The Main Menu

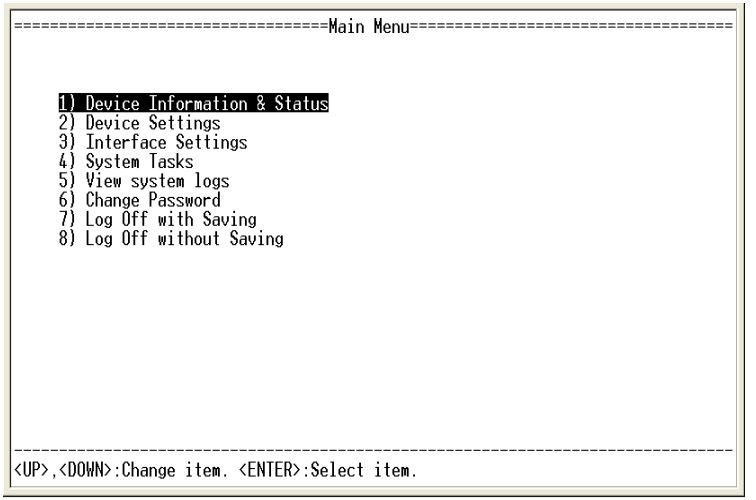


TABLE 6-1. The Main Menu item descriptions

MENU ITEMS	DESCRIPTION
1) Device Information and Status	View product information and monitor CPU and memory usage.
2) Device Settings	Modify the device host name, IP address, subnet mask, and the network default gateway address and DNS servers. You can also register to Trend Micro Control Manager for centralized management.
3) Interface Settings	By default, Threat Discovery Appliance automatically detects the network speed and duplex mode. However, if any issues with the connection arise, you can manually configure these settings.

MENU ITEMS	DESCRIPTION
4) System Tasks	Roll back to the previous update, import and export the configuration file, import the HTTPS certificate, perform a diagnostic test, or restart the device.
5) View System Logs	View the security risks and incidents as they happen.
6) Change Password	Change the root password.
7) Log Off with Saving	Log off from the Preconfiguration Console after saving the changes.
8) Log Off without Saving	Log off from the Preconfiguration Console without saving the changes.

Preconfiguration Console Navigation

- To navigate the Preconfiguration console, type the index number of the desired selection and press the ENTER key.
- To return to the **Main Menu**, press the `Esc` key.
- To skip an entry or keep the current value, press the Up and Down keys.
- To go back to the top of a menu tree or to exit the Preconfiguration console from the **Main Menu**, enter the `Esc` key.

Viewing Device Information and Status

View device information and status to monitor the performance of the following:

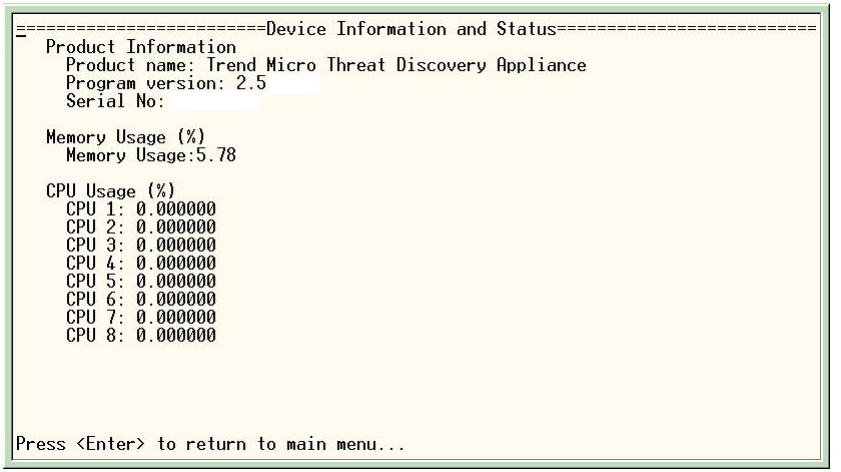
TABLE 6-2. Device information

ITEM	DESCRIPTION
Product Information	Shows the product name, program version, and serial number.
Memory	The percentage of RAM currently in use.
CPUs	The percentage of CPU resources currently in use for physical CPUs (8 logical CPUs).

To view device information:

1. Log on to the Preconfiguration console. The Main Menu appears.
2. Type **1** to select **Device Information & Status** and press the ENTER key. The Device Information and Status screen appears.

FIGURE 6-3. The Device Information and Status screen



Configuring Device Settings

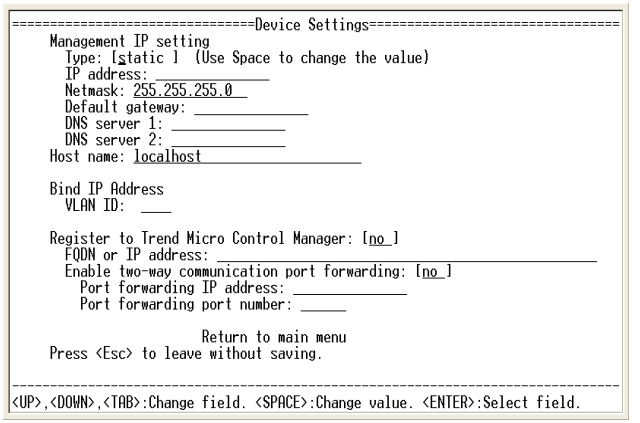
You can modify device network settings using the Preconfiguration console or the

product console.

To modify network settings:

1. Log on to the Preconfiguration console. The Main Menu appears.
2. Type **2** to select **Device Settings** and press the ENTER key. The Device Settings screen appears.

   FIGURE 6-4. The Device Settings screen



3. Change the IP address setting:

   To use dynamic IP address:

   a. Use the space bar to change the IP address option from **static** to **dynamic**.

   To use static IP address:

   a. Use the space bar to change the IP address setting from **dynamic** to **static**.

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

4. Change the **Host name**:

   a. Navigate to the **Host name** option.

   b. Specify the new host name.

5. (Optional) Bind the IP Address:

a. Navigate to the **Bind IP Address** option.

b. Specify a **VLAN ID**. Press the ENTER key.

6. Register to Trend Micro Control Manager:

Note: Registration is optional. You can use the product console to register to Control Manager at a later time.

a. Use the down arrow to bring the cursor to **Register to Control Manager** and then use the spacebar to change the option to **[yes]**.

b. Type the Control Manager server IP address in the **FQDN** or **IP address** field.

c. Use the spacebar to change the **Enable two-way communication port forwarding** option from **no** to **yes**.

d. Type the port number and IP address of your router or NAT device server in the **Port forwarding IP address** and **Port forwarding port number** fields. 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. For more information on NAT, refer to the *Trend Micro Control Manager Administrator's Guide*.

7. Navigate to **Return to main menu**. Press the ENTER key to return to main menu.
8. Navigate to **7) Log Off with Saving**. Press the ENTER key to save the settings.

Modifying Interface Settings

By default, Threat Discovery Appliance automatically detects the network speed and duplex mode, 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.

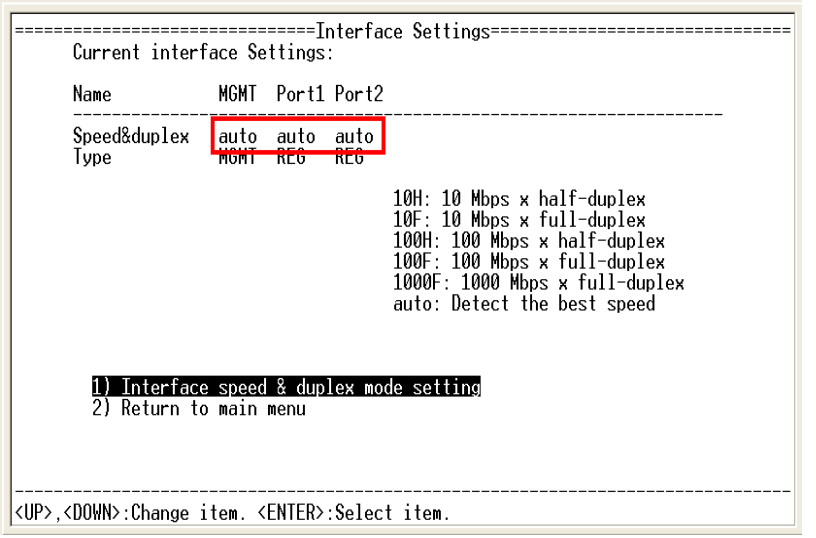
Tip: To maximize throughput, Trend Micro recommends full-duplex mode.

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.

To modify interface settings:

1. Log on to the Preconfiguration console. The Main Menu appears.
2. Type **3** to select **Interface Settings** and press the ENTER key. The Interface settings of the Management and Data ports appear.

FIGURE 6-5. The Interface Settings screen



3. To change the interface settings, type **1** and press the ENTER key.
4. Press the up and down arrow keys to move to the MGMT, Port1, or Port2 settings.
5. Use the space bar to change the values of the settings.

Tip: The available options are shown beneath the field settings.

6. Type **2** and press the ENTER key to **Return to the main menu**. Press the ENTER key to return to main menu.

7. Navigate down to **7) Log Off with Saving**. Press the ENTER key to save the settings.

Performing System Tasks

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 device, use the System Tasks screen.

Tip: Importing and exporting the configuration file is also available from the product console.

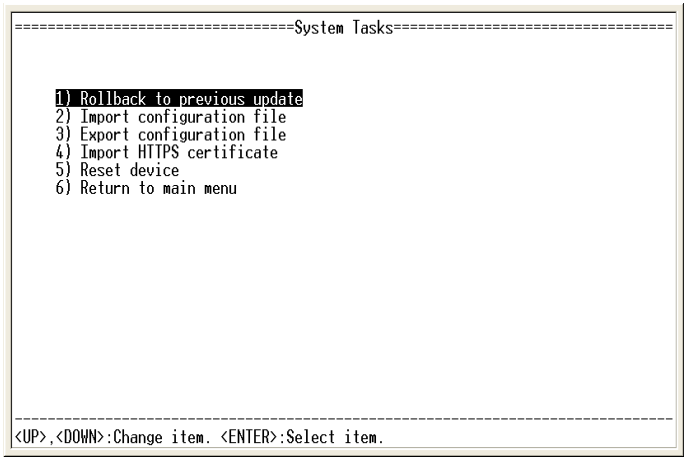
Roll back to the Previous Update

If the update is not compatible with your device, 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** then press the ENTER key. The System Tasks screen appears.

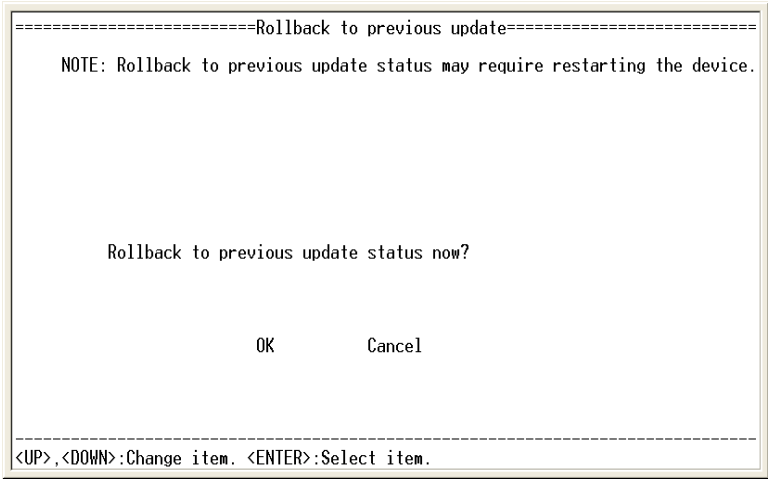
FIGURE 6-6. The System Tasks screen



3. Type **1** then press the ENTER key. The Rollback to previous update screen appears.

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

FIGURE 6-7. The Rollback to previous update screen



4. Select **OK** and press the ENTER key.
5. The device rolls back to the previous updates.

Importing the Configuration File

If Threat Discovery Appliance encounters errors with the current settings, you can restore the configuration and database from a backup file.

WARNING! Export your current configuration settings before importing the backup configuration file (see *Exporting the Configuration File* on page 6-15).

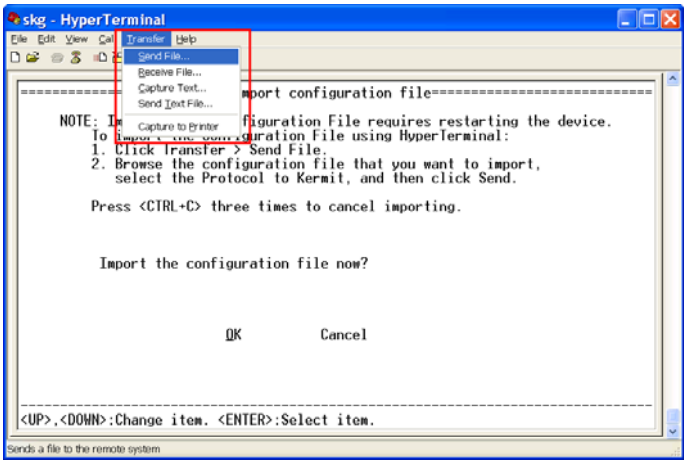
To import the backup configuration file:

1. Log on to the Preconfiguration console. The Main Menu appears.
2. Type **4** then press the ENTER key. The System Tasks screen appears.

3. Type **2** then press the ENTER key. The Import configuration file screen appears.
4. From the HyperTerminal menu, click **Transfer > Send File**.

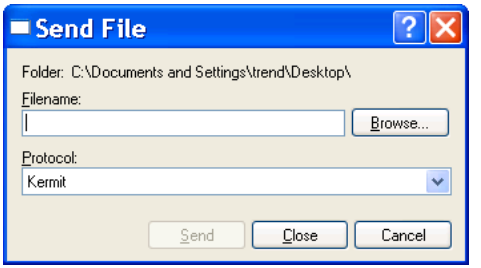
Note: Send file means you send the file to the device before you can import it.

FIGURE 6-8. Preconfiguration console send file screen



5. Browse to the configuration file you want to import.

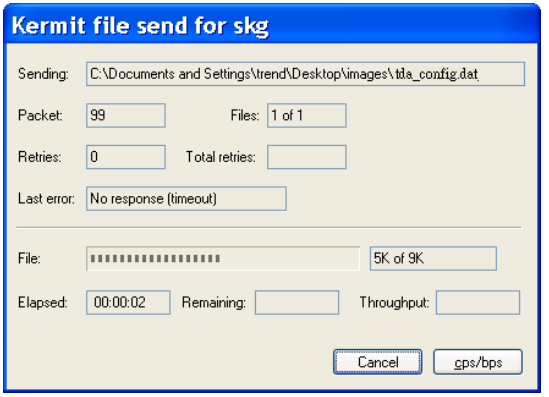
FIGURE 6-9. Send file screen



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

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

FIGURE 6-10. Kermit file send screen



7. The device imports the configuration file and uses the settings from the file.

Exporting the Configuration File

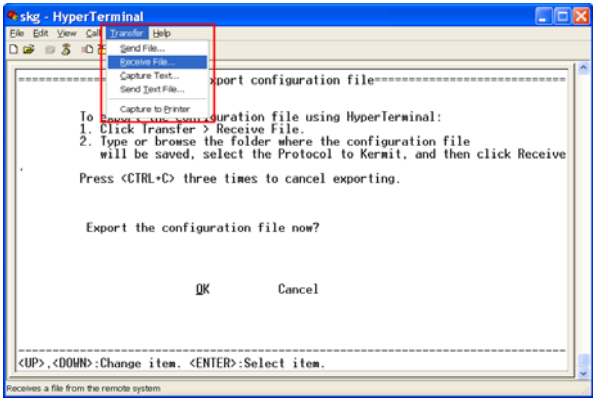
Regularly back up the configuration files to ensure that you use the latest configuration settings when importing.

To export the configuration file:

1. Log on to the Preconfiguration console. The Main Menu appears.
2. Type **4** then press the ENTER key. The System Tasks screen appears.
3. Type **3** then press the ENTER key. The Export configuration file screen appears.
4. From the HyperTerminal menu, click **Transfer > Receive File**.

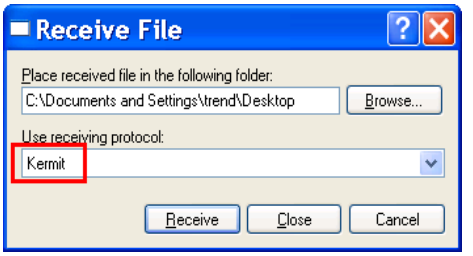
Note: Receive file means receiving the file from the device before exporting.

FIGURE 6-11. Preconfiguration console receive file screen



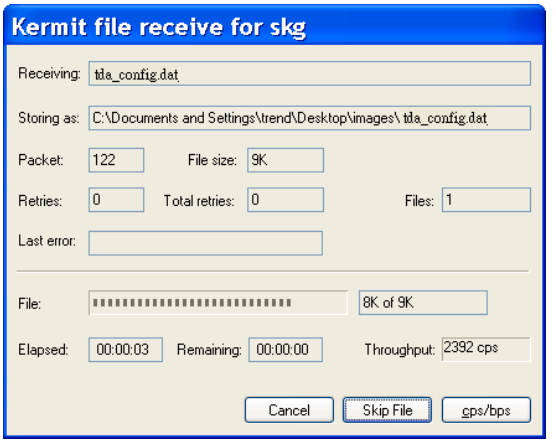
5. Browse to the configuration file you want to export.

FIGURE 6-12. Receive file screen



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

FIGURE 6-13. Kermit file receive screen



7. The device exports the configuration settings into a `.dat` file.

Tip: Rename the exported configuration files to keep track of the latest configuration files.

Importing the HTTPS Certificate

You can import the HTTPS certificate to ensure connection to the correct server. Replace the HTTPS Certification from the product console's HTTPS Certificate screen.

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

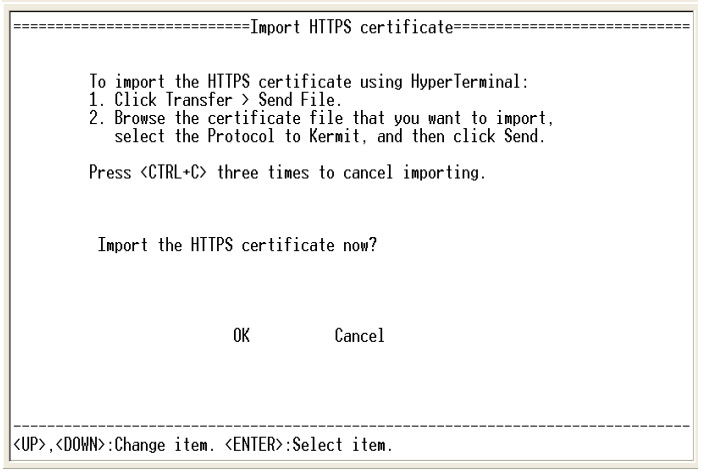
```
openssl req -new -x509 -days 365 -nodes -out FILE_NAME.pem -keyout
FILE_NAME.pem
```

To import the HTTPS certificate:

1. Log on to the Preconfiguration console. The Main Menu appears.
2. Type **4** then press the ENTER key. The System Tasks screen appears.

3. Type **4** then press the ENTER key. The Import HTTPS certificate screen appears.

FIGURE 6-14. The Import HTTPS Certificate screen



4. From the HyperTerminal menu, click **Transfer > Send File**.
5. Browse to the configuration 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 or hardware issues.

To perform the diagnostic test:

1. Log on to the Preconfiguration console. The Main Menu appears.
2. Type **4** then press the ENTER key. The System Tasks screen appears.
3. Type **5** then press the ENTER key. 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 the ENTER key.

8. After Threat Discovery Appliance restarts, open the captured log to view the log result.

Restarting the Device

To restart Threat Discovery 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 device remotely.

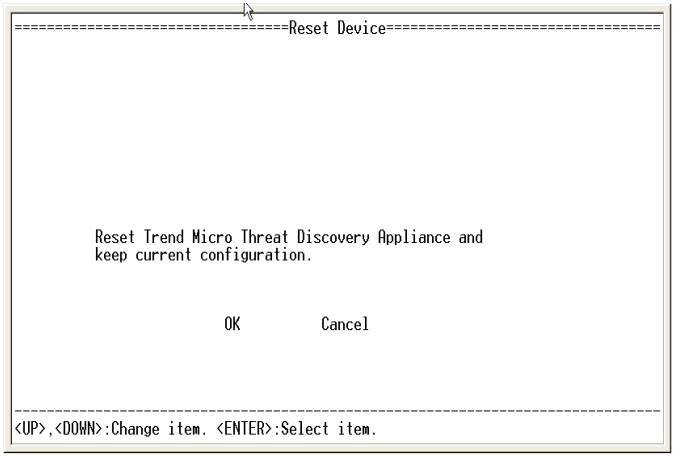
Note: The device automatically starts when power is restored after a power failure. This means you do not have to physically turn the device back on. However, shutting down the device before a power failure means the device will not automatically start when power is restored.

To restart the device:

1. Log on to the Preconfiguration console. The Main Menu appears.
2. Type **4** then press the ENTER key. The System Tasks screen appears.
3. Type **6** then press the ENTER key. The Reset Device screen appears.

4. Under **Reset Trend Micro Threat Discovery Appliance and keep current configuration**, navigate to **OK** and press the ENTER key.

FIGURE 6-15. The Reset Device screen



5. The device restarts.

Viewing the System Logs

View the logs in the Preconfiguration console.

Note: The log format in the Preconfiguration console displays the logs. For more organized and configurable logs, use the product console feature, Detection Log Query (See *Viewing Detection Log* on page 5-24).

To view the system logs in the Preconfiguration console:

1. Log on to the Preconfiguration console. The Main Menu appears.
2. Type **5** then press the ENTER key. 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.

FIGURE 6-16. An example of a System log

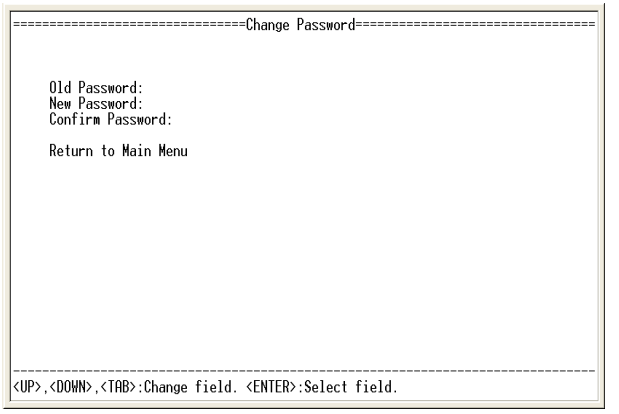
Changing the Root Password

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** then press the ENTER key. The Change Password screen appears.

FIGURE 6-17. The Change Password screen



3. Type the old and new passwords.
4. Confirm the new password.
5. Return to the main menu to save the settings.

Logging off from the Preconfiguration Console

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

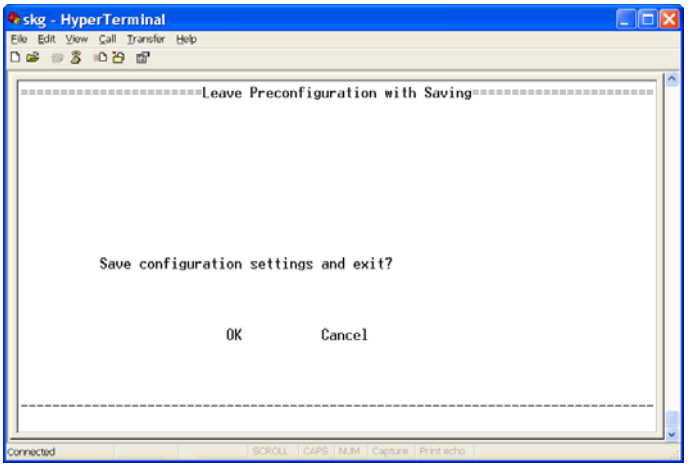
- Log off with Saving
- Log off without Saving

To log off and save:

Note: Some tasks, such as changing the password and resetting the device, 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** then press the ENTER key. The Leave Preconfiguration with Saving screen appears.
3. Under **Save configuration settings and exit?**, navigate to **OK** and press the ENTER key.

FIGURE 6-18. The Leave Preconfiguration with Saving screen

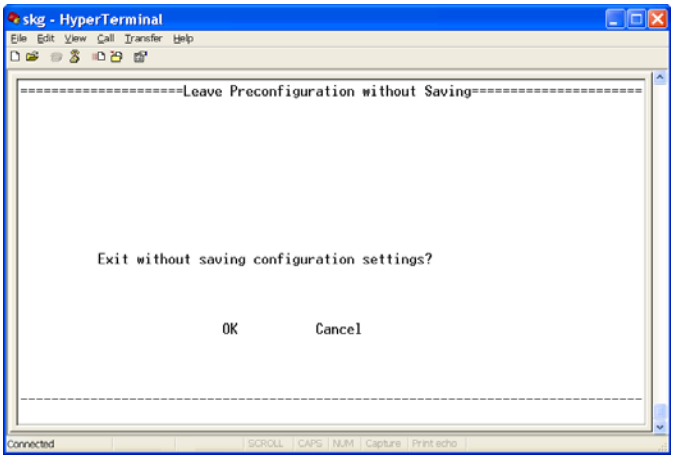


To log off without saving:

1. After making any changes to the configuration settings, return to the main menu.
2. Type **8** then press the ENTER key. The Leave Preconfiguration without Saving screen appears.

3. Under **Exit without saving configuration settings?**, navigate to **OK** and press the ENTER key.

FIGURE 6-19. The Leave Preconfiguration without Saving screen



Rescuing Threat Discovery Appliance

Rescuing Threat Discovery Appliance means reinstalling the Threat Discovery Appliance application and reverting to saved or default settings. As an alternative, you can use the Web-based product console to rescue the device (see *Backup/Restore* on page 4-28) or update the firmware (see *Updating the Firmware* on page 4-31).

Application Rescue Overview

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

Rescuing the application is not the same as applying a patch:

- Rescuing—replaces application files and keeps or restores the default settings.
- Applying a patch—updates the existing application files to enhance features.

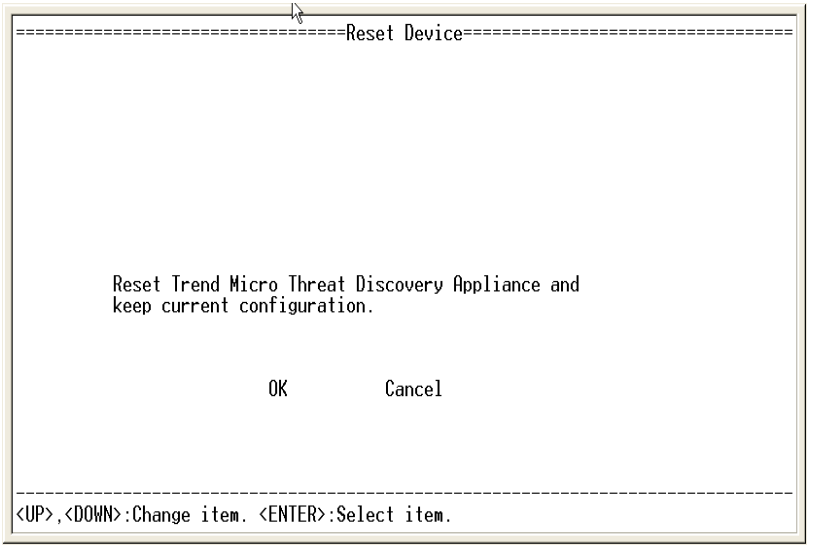
WARNING! **Before rescuing the application, create a backup of your settings (see *Backing Up Device Configuration Settings* on page 4-28).**

To enter rescue mode:

1. Log on to the Preconfiguration console through a serial connection to the management port (see *Using the Preconfiguration Console* on page 6-2).
2. Type **4** then press the ENTER key. The System Tasks screen appears.

3. Type **5** then press the ENTER key. The Reset Device screen appears.

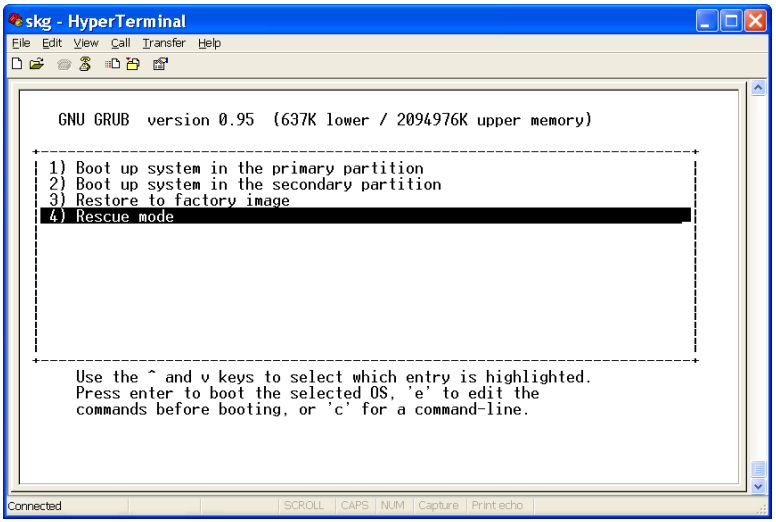
FIGURE 6-20. The Reset Device screen



4. The device restarts.

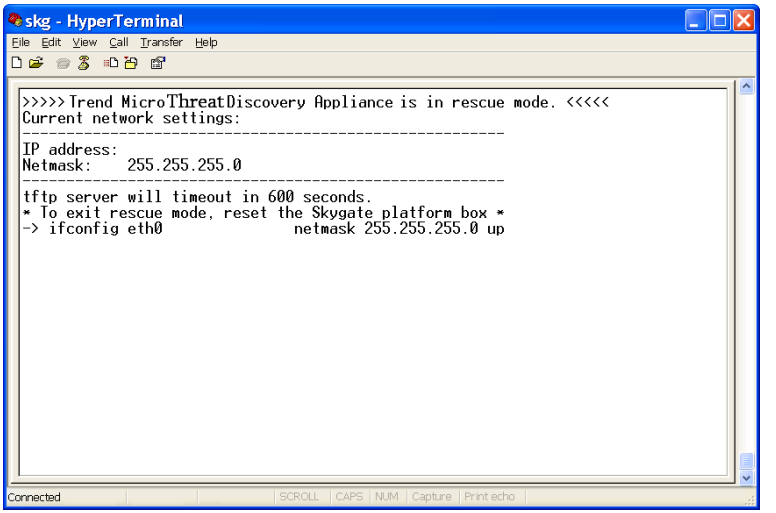
5. When the *Press the ESC button* message appears in the boot screen, press ESC immediately. The boot menu appears.

FIGURE 6-21. The Boot menu



6. Type **4** then press the ENTER key. The Threat Discovery Appliance rescue mode screen appears.

FIGURE 6-22. The Threat Discovery Appliance rescue mode screen



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

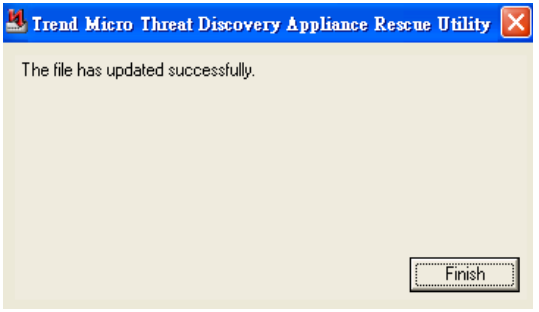
WARNING! Ensure you are in Rescue mode before using the Rescue Tool.

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 device.

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

FIGURE 6-23. File upload successful



11. In HyperTerminal, type **Y** to migrate the previous configuration files. press the ENTER key to continue. Threat Discovery Appliance starts migrating the configuration files.

FIGURE 6-24. The configuration file migration screen

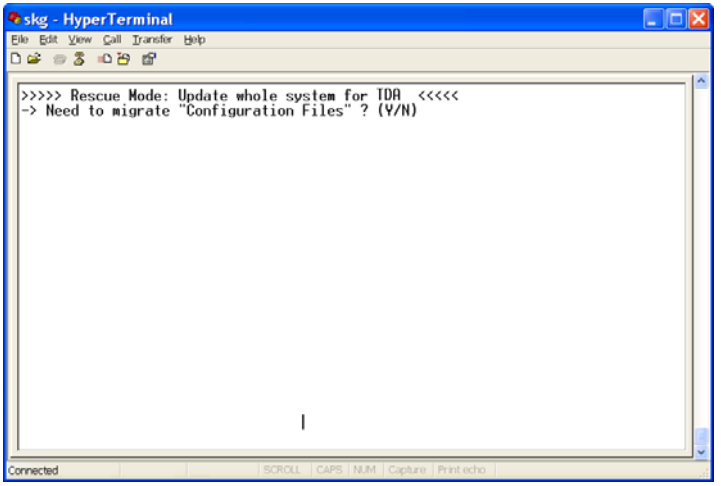
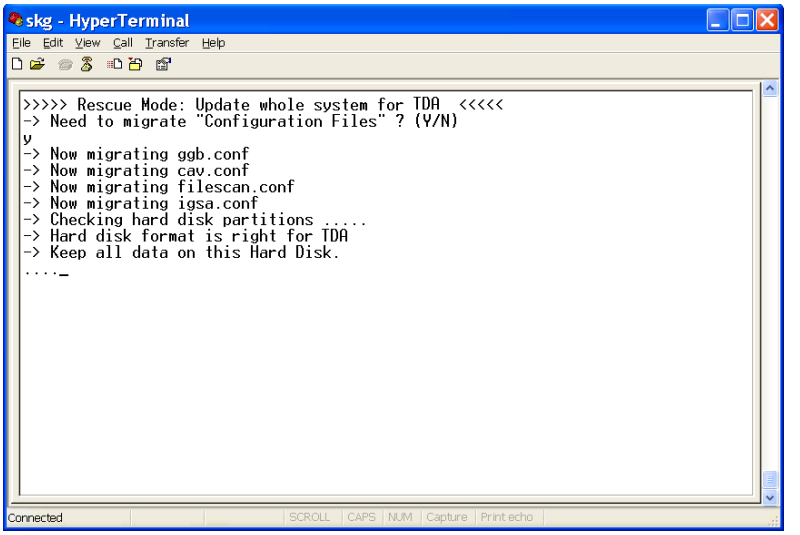


FIGURE 6-25. Configuration migration screen



12. After migration, open the Preconfiguration console and configure the Threat Discovery Appliance network settings (see *Configuring Device Settings* on page 6-7).

Chapter 7

FAQs and Technical Support

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

The topics discussed in this chapter are:

- *Frequently Asked Questions (FAQs)* on page 7-2
- *Trend Micro Technical Support* on page 7-6

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 this device 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 for Threat Management Services 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 a device to more than one Control Manager server. To register a device to a Control Manager server, refer to *Registering to Control Manager* on page 4-25.

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 temporarily disconnect (30 seconds) the device. 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 used the wrong password three times in a row, the device will lock for 30 seconds before you can try to log on again. Wait 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 for Threat Management Services Portal, you need to configure the firewall to allow Ports 80, 22 or 443 traffic from Threat Discovery Appliance.

I am unable to register to Threat Management Services Portal, what can I do?

Ensure the following:

- all the Threat Management Services Portal log on 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 problem persists, consult your support provider.

Updating the Device

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 the device?

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 device every 2 hours.

Does the device 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 device.

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

Updating Threat Discovery Appliance components follows the device constraints. This means that when updating components, the device updates the software first. Restart the device and update the Network Content Inspection Engine. Restart the device 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: *Quick Start Guide*, *Administrator's Guide*, readme file, Safety sheet, Hardware maintenance sheet and help files for Threat Discovery Appliance.

I have questions/issues with the documentation. How can I provide feedback to Trend Micro?

Trend Micro is always seeking 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

Trend Micro Technical Support

Registering Threat Discovery Appliance entitles you to technical support, component downloads, and program updates for one year, after which you must purchase renewal maintenance.

Contacting Trend Micro

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

http://www.trendmicro.com/en/about/contact/overview.htm

Note: The information in this Web site is subject to change without notice.

The Trend Micro Security Information Center

Comprehensive security information is available over the Internet, free of charge, in the Trend Micro Security Information Web site:

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

TABLE 7-1. Virus Encyclopedia contents

VISIT THE SECURITY INFORMATION SITE TO:	
Read the Weekly Virus Report	These reports include a listing of threats expected to trigger in the current week, and describes the current weeks 10 most prevalent security risks/threats around the globe.
View a Virus Map	The Virus Map shows the top 10 threats around the globe.
Consult the Virus Encyclopedia	The Virus Encyclopedia is a compilation of known threats including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the threat, as well as information about computer hoaxes.
Download test files	The European Institute of Computer Anti-virus Research (EICAR) files help you test whether your security product is correctly configured.
Read general virus information	-Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other threats -Trend Micro *Safe Computing Guide* -A description of risk ratings to help you understand the damage potential for a threat rated Very Low or Low vs. Medium or High risk -A glossary of virus and other security threat terminology
Download comprehensive industry white papers	View Trend Micro white papers containing information and research results.
Subscribe to Trend Micro's Virus Alert service	Subscribe to learn about outbreaks as they happen, and Weekly Virus Reports
Learn about free virus update tools available to Web masters	Use these tools to add virus updates to your Web sites.

Read about Trend-Labs[SM]	TrendLabs is Trend Micro's global antivirus research and support center

Contacting Technical Support

You can contact Trend Micro through fax, phone, and email, or visit us at:

http://www.trendmicro.com

Speeding Up Your Support Call

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

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

The Trend Micro Knowledge Base

Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do. New solutions are added daily.

Also available in Knowledge Base are product FAQs, important tips, preventive antivirus advice, and regional contact information for support and sales.

Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

http://esupport.trendmicro.com/

If you are unable to find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question using an email message. Response time is typically 24 hours or less.

Sending Suspicious Files to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, contact your support provider or visit the Trend Micro Submission Wizard URL:

http://subwiz.trendmicro.com/SubWiz

Click the link under the type of submission you want to make.

Note: Submissions made through the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you submit your case, an acknowledgement screen displays. This screen also displays a case number. Make note of the case number for tracking purposes.

If you prefer to communicate by email message, send a query to the following address:

virusresponse@trendmicro.com

In the United States, you can also call the following toll-free telephone number:

`(877) TRENDAV, or 877-873-6328`

About TrendLabs

TrendLabs^{SM} is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA, to mitigate virus outbreaks and provide urgent support.

TrendLabs' modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000—one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.

Appendix A

Deploying Threat Discovery Appliance

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

The topics discussed in this chapter are:

- *Deployment Considerations* on page 2
- *Deployment Scenarios* on page 2

Deployment Considerations

Consider the following before deploying Trend Micro™ 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.

- **Device 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.

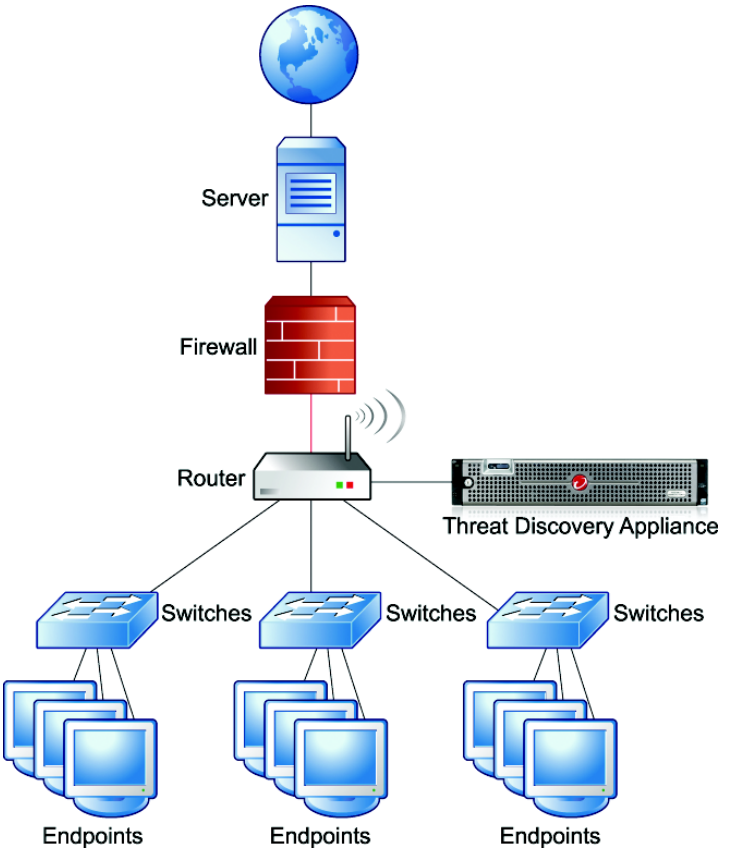
Deployment Scenarios

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.

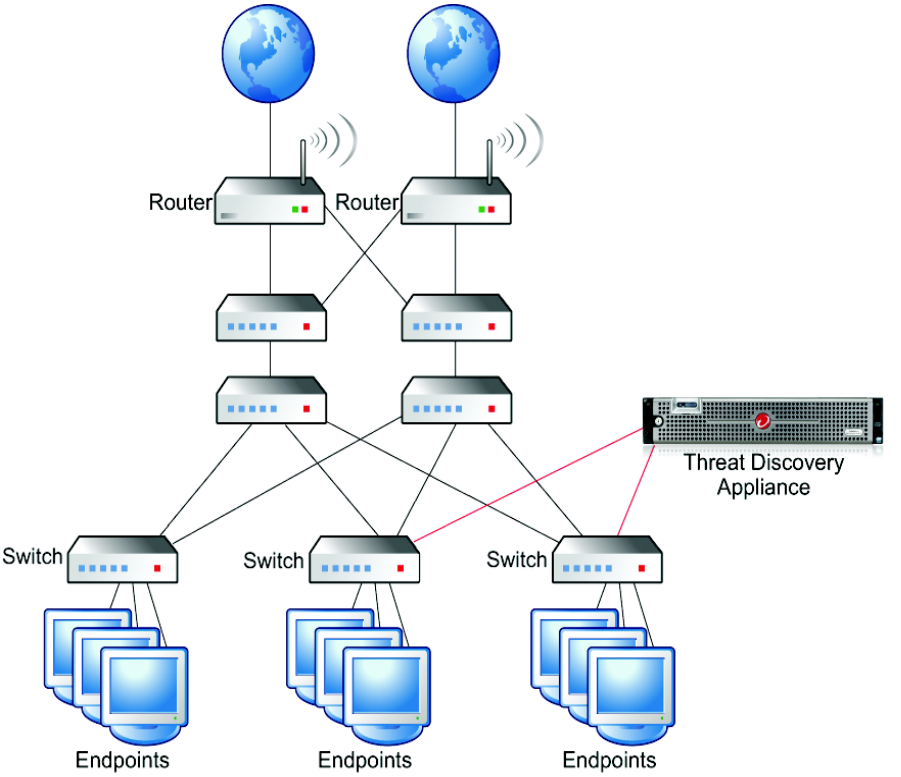
FIGURE A-1. Threat Discovery Appliance single port monitoring



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.

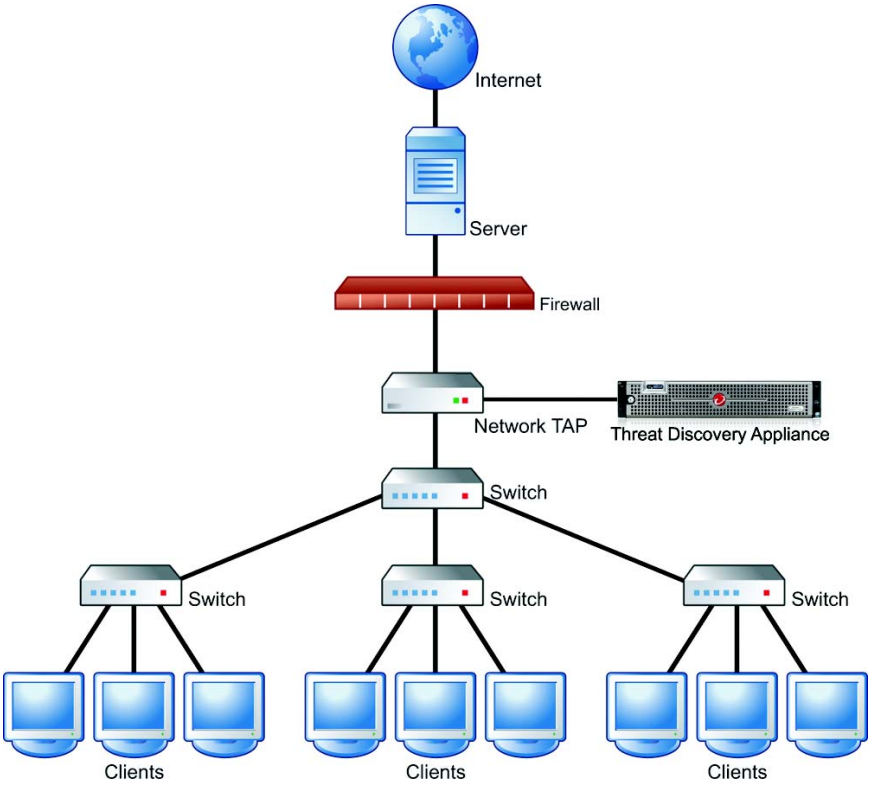
FIGURE A-2. Threat Discovery Appliance dual port monitoring



Network TAP

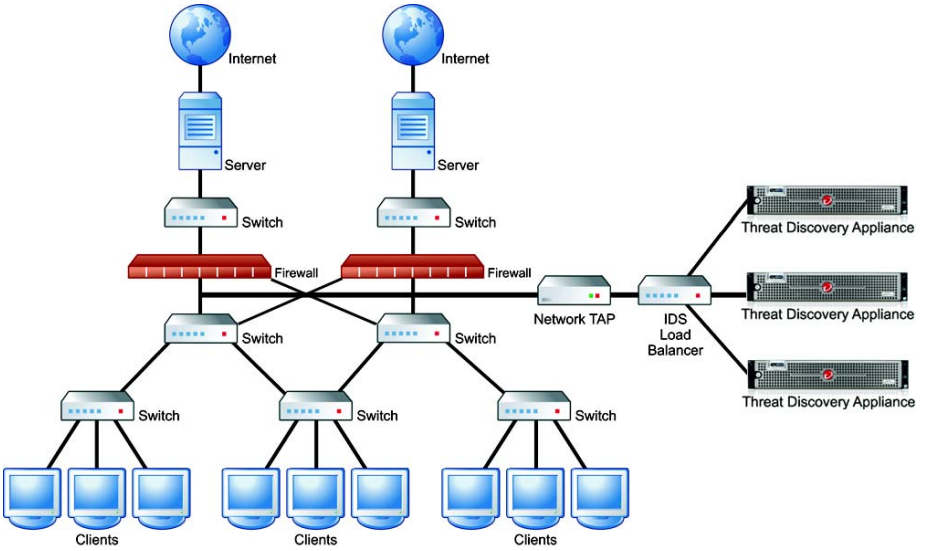
Network TAPs can monitor the data flowing across the network from interconnected switches, routers, and computers. In this scenario, connect the Threat Discovery Appliance device to a network TAP.

FIGURE A-3. Single Threat Discovery Appliance device connected to a network TAP



Additionally, use an Intrusion Detection System load balancer for better performance when deploying multiple Threat Discovery Appliance devices.

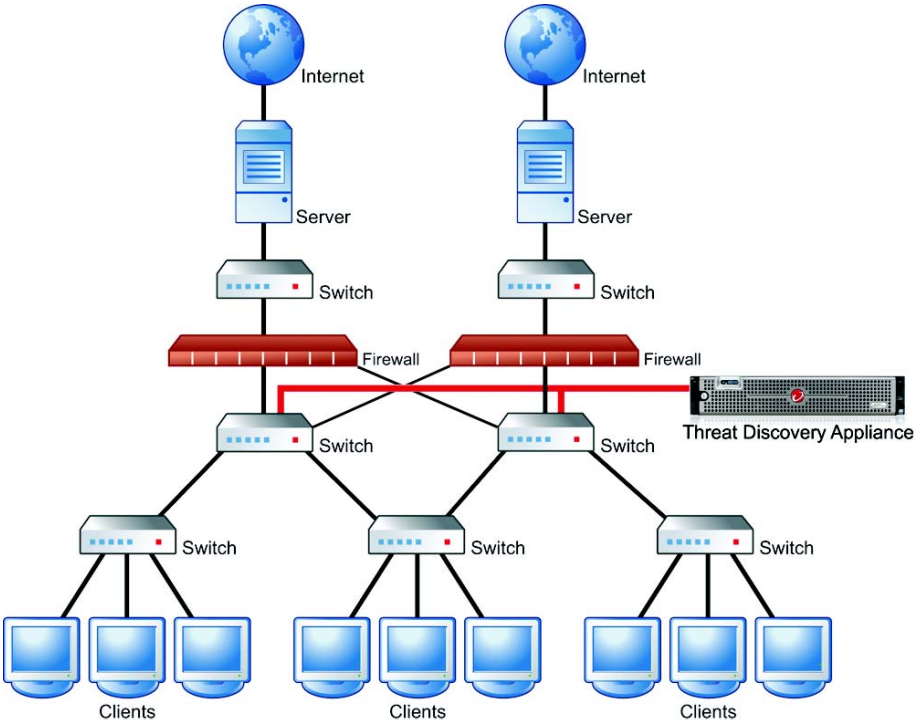
FIGURE A-4. Multiple Threat Discovery Appliance devices connected to a network TAP



Redundant Networks

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

FIGURE A-5. Redundant network monitoring



Specific VLANs

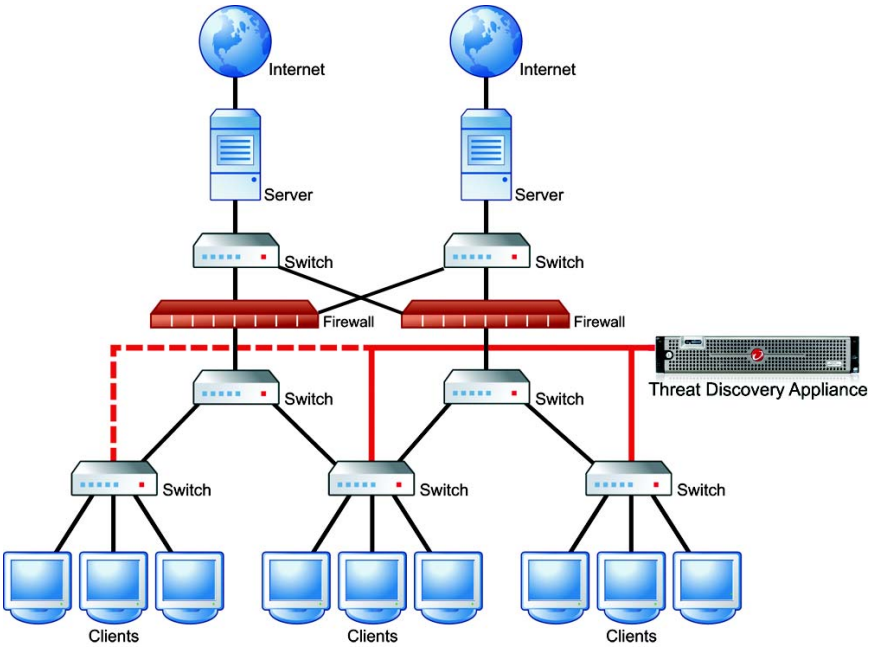
Some enterprise environments limit port scanning to specific VLANs. This can save some bandwidth and can be less resource intensive. In this scenario, the Threat Discovery Appliance device connection to the switches remains the same but the mirror configuration should be VLAN based.

Remote Port or VLAN Mirroring

Use remote mirroring for the following scenarios:

- Monitoring more than 6 switches
- Local switch does not have enough physical ports
- Port speed on local switches do not match (GB/MB)

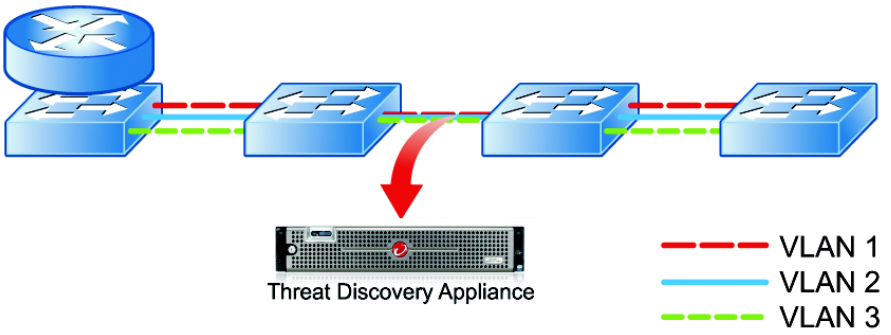
FIGURE A-6. Remote port or VLAN mirroring



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 direction

FIGURE A-7. Mirroring trunk links



Appendix B

Glossary

This glossary describes terms used in this document or the online help.

TABLE B-1. Glossary

TERM	EXPLANATION
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 Web site, 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

TERM	EXPLANATION
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.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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

TERM	EXPLANATION
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

TERM	EXPLANATION
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 Web site 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 Web site 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

TERM	EXPLANATION
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

TERM	EXPLANATION
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

TERM	EXPLANATION
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 a .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

TERM	EXPLANATION
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. A minority 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

TERM	EXPLANATION
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

TERM	EXPLANATION
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

TERM	EXPLANATION
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

TERM	EXPLANATION
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.

TABLE B-1. Glossary

TERM	EXPLANATION
LCM console	Also referred to as the LCD module. It is composed of the LCD and the Control Panel, which is located on the Trend Micro Threat Discovery Appliance front panel.
Liquid Crystal Display (LCD)	A 5x7 dot display LCD on the Threat Discovery Appliance front panel capable of displaying 2x16 character messages.
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.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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 Trend Micro™ Threat Discovery Appliance.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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.

TABLE B-1. Glossary

TERM	EXPLANATION
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.
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

Numerics

20 recent security risks/threats 5-6

A

Activation code 3-8
ActiveUpdate server 3-11
Administrator's Guide x
Appliance health
  critical 5-3
  normal 5-2
  warning 5-2
Appliance host name 3-5
Application filters 4-9
  instant messaging 4-10
  peer-to-peer 4-10
  streaming media 4-10
Application filters log query 5-26
Application requirements 2-4
Audience x

B

Backup
  about 4-28
  device configuration settings 4-28
  network configuration 4-7

C

Cable routing 2-24
Cable tray 2-23
Cable-management arm
  installing 2-23
Change password 3-4, 6-21
Components
  firmware 3-10
  intellitrap exception pattern 3-10
  intellitrap pattern 3-10
  network content correlation engine 1-4, 3-10
  network content correlation pattern 3-10
  network content inspection engine 1-4, 3-10
  network content inspection pattern 3-10
  pattern file 3-10
  scan engine 1-3, 3-10
  spyware pattern file 3-10
Configuration settings
  device 4-28
  network 4-7
Contacting Trend Micro 7-6
Contents listed
  RapidRails kit 2-10
Control Manager 4-25
Control Manager registration 6-9

D

Default gateway 3-2
Default settings 4-30
Delivery options 5-8
Deployment
  considerations A-2
  dual port A-4
  mirroring trunk links A-9
  network tap A-5

redundant networks A-7
remote port A-8
single port A-3
specific vlan A-8
vlan mirroring A-8
Detected files 4-13
Detection Exclusion List 1-7
Detection exclusion list 4-15
about 4-15
outbreak containment services 4-17
potential threat detections 4-15
Detection log query 5-24
Detections in past 24 hours 5-5
Device configuration settings
about 4-28
restore 4-29
Device information and status 6-6
Device name 3-5
Device requirements 2-1
Diagnostic test 6-18
Documentation
conventions xi
download i
FAQs 7-5
feedback ii, 7-5
included x
Doors
removing 2-11
replacing 2-27
Dual port monitoring A-4
Duplex mode 6-9

E

Enhanced Mitigation 1-8
Ethernet port 2-2—2-3

F

FAQs 7-2
Firmware 3-10
Four-post rack kit
RapidRails kit contents 2-10
tools and supplies 2-9
Frequently asked questions 7-2

G

General rack installation 2-8
Glossary B-1
Glossary of security threat terms 7-7

H

Hardware requirements 2-3
High network traffic usage notifications 5-15
High risk client notifications 5-13
High risk clients 5-20
Host name 3-2

I

IM 4-10
Indicators
about 5-2
appliance health 5-2
network flow 1-7, 5-3
risk meter 5-2
Installing 2-23
cable tray 2-23
cable-management arm 2-23
four-post rack kit 2-17
RapidRails mounting rails 2-17
system in four-post rack 2-20
VersaRails mounting rails 2-19, 2-21
Instant Messaging 4-10
Integration
about 4-23
Control Manager 1-6
control manager 4-25
leakproof 1-8
mitigation devices 4-23
mitigation servers 1-6, 1-8
network viruswall 1-6, 1-8

threat management services 1-8
IntelliTrap 1-4
IntelliTrap exception pattern 3-10
IntelliTrap pattern 3-10
Interface speed and duplex mode settings 6-9
IP address 3-2
IP Address settings 3-4
ISO 9002 Certification-see TrendLabs 7-10

K

Kit contents
RapidRails 2-10
Knowledge Base 7-8
Known security risks notifications 5-12
Known security risks/threats 5-5

L

LCD 2-27
LCM 2-27
License
activation 3-8
renewal 3-8
Liquid crystal display module 2-27
Log maintenance 5-29
Logs
about 5-18, 5-24
application filter 5-18
application filters log query 5-26
detection log query 1-8, 5-24
detection logs 5-18
maintenance 5-29
syslog server settings 5-28
system 5-18
system log query 5-27

M

Management console 3-3
Marking rack
four-post rack kit 2-11
Minimum requirements 2-2
Mitigation devices 4-23
Mitigation Exclusion List 1-7
Mitigation settings 4-24
Monitored networks 4-2
Mounting the device 2-11
Multi-layered files 1-3
Multi-packed files 1-3

N

Network configuration
about 4-2
detection exclusion list 4-15
monitored networks 4-2
registered domains 4-4
registered services 4-6
Network configuration settings
about 4-7
export 4-8
import 4-8
Network content correlation
engine 3-10
pattern 3-10
Network content inspection
engine 3-10
pattern 3-10
Network flow
critical 5-3
normal 5-3
Network settings
default gateway format 3-2
host name format 3-2
IP address format 3-2
subnet mask format 3-2
VLAN ID format 3-2
Network time protocol 3-6
Network Virus Scan 1-4
Network VirusWall 4-23
Notifications
about 5-8
delivery options 5-8

high network traffic usage 5-15
high risk clients 5-13
known security risks 5-12
potential security risks 5-10
NTP 3-6
Number of incidents
about 5-19
detection type 5-20
protocol 5-20
time of day 5-20

O

Offline Monitoring 1-5
Online Help x
Outbreak Containment Services 1-7, 4-9, 4-17, 5-6

P

P2P 4-10
Password 3-3—3-4, 6-21
Pattern file 3-10
Peer-to-Peer 4-10
Port
multiple support 1-6
Potential Risk File 1-4
Potential security risks notification 5-10
Potential security risks/threats 5-5
Potential threat detections exclusions list 4-15
Power supplies
about 2-5
Powering off 2-6
Preconfiguration console 6-2
changing root password 6-21
device information and status 6-6
import configuration file 6-13
import HTTPS certificates 6-17
interface speed and duplex mode settings 6-9
log off 6-22
navigation 6-6
overview 6-4
rollback 6-11
system logs 6-20
system tasks 6-11
Product console 3-3
Protocol
support 1-5
Proxy settings 3-7

Q

QSG x
Quick Start Guide x

R

Rack installation 2-8
Rack mount precautions 2-8
Rack mounting 2-7, 2-11
Rack unit 2-12
RapidRails 2-8
kit contents 2-10
Readme File x
Recent alerts 5-6
Register to Trend Micro Control Manager 6-9
Registered domains 4-4
Registered services 4-6
Replacing rack doors 2-27
Reports
about 5-18
delivery settings 5-23
high risk clients 5-20
number of incidents 5-19
traffic 5-21
Rescue mode 6-25
Rescuing the device 6-25
Reset device settings 4-30
Restart
device 4-34
services 4-34
Restarting the device 6-19
Risk meter 5-2

critical risk 5-2
low risk 5-2
normal 5-2
Risk ratings
security information center 7-7
Rollback update 6-11
Root password 6-21
Routing cables 2-24

S

SaaS 4-20
Safe computing guide 7-7
Safety
information 2-8
Scan engine 1-3, 3-10
Security information center 7-6
EICAR test file 7-7
glossary of security threat terms 7-7
risk ratings 7-7
safe computing guide 7-7
TrendLabs 7-8
URL 7-6
virus alert 7-7
Virus Encyclopedia 7-7
virus primer 7-7
webmaster tools 7-7
weekly virus report 7-7
Security risk meter 4-19, 5-5
Sending suspicious files to Trend Micro 7-9
Setup Guide 1-7
Single port monitoring A-3
Software as a service 4-20
Spyware pattern file 3-10
Streaming media 4-10
Submission wizard 7-9
Subnet mask 3-2
Summary
20 recent security risks/threats 5-6
detections in past 24 hours 5-5
outbreak containment services 5-6
potential security risks/threats 5-5
recent alerts 5-6
security risk meter 5-5
system events 5-7
Summary screen 5-4
Suspicious files 7-9
Syslog server settings 5-28
System events 5-7
System log query 5-27
System logs 6-20
System Maintenance
remote 1-6
System maintenance
about 4-33
restart device 4-34
restart services 4-34
System requirements 2-2
System time settings 3-6

T

Technical support 7-8
Threat Detail 1-8
Threat detections
about 4-9
block traffic 4-9
outbreak containment services 4-9
Threat Discovery Appliance
about 1-2
features 1-2
monitoring
dual port monitoring A-4
single port monitoring A-3
Threat Discovery Appliance components 3-10
Threat Discovery Appliance rescue tool 6-28
Threat Management Services 4-20
Threshold settings
about 4-18
critical risk 4-18

low risk 4-18
TMCM 4-25
Tools and supplies
four-post rack kit 2-9
Traffic 5-21
Trend Micro
contacting 7-6
TrendLabs 7-8—7-9
True File Type 1-3
Turning off the device 2-6

U

Update settings 3-11
Updates
about 3-9
ActiveUpdate server 3-11
firmware 4-31
manual 3-9, 3-12
scheduled 3-9, 3-13
settings 3-11
source 3-11
Updating
FAQs 7-4
URLs
Knowledge Base 7-8
Submission wizard 7-9

V

VersaRails 2-8
installing 2-19, 2-21
Vertical rails
marking 2-11
one rack unit 2-12
Virus alert service 7-7
Virus Encyclopedia 7-7
Virus pattern file 3-10
Virus primer 7-7
Virus Scan Engine 1-3
Virus scan engine 3-10
VLAN ID 3-2
VMware 1-6

W

Web console 3-3
Web console URL 2-4
Web-based console 3-3
WebHelp x
Webmaster tools 7-7
Weekly virus report 7-7
What's New
configuration 1-7
hardware 1-6
integration 1-8
logs 1-8
software 1-6