3.2 Deep Discovery Inspector
Administrator's Guide
Breakthrough Protection Against APTs and Targeted Attacks
The Administrator’s Guide for Trend Micro™ Deep Discovery Inspector is intended to introduce the main features of the product, provide deployment information for your production environment, and provide information on configuring and using the product. Read through this document prior to deploying or using the product.

Detailed information about how to use specific features are available in the online help file and the online Support portal at the Trend Micro website.

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

http://www.trendmicro.com/download/documentation/rating.asp
Table of Contents

Chapter 1: Introducing Deep Discovery Inspector

About Deep Discovery Inspector .......................................................... 1-2
Threat Management Capabilities ...................................................... 1-2
Deep Discovery Inspector Features ................................................. 1-3
Deep Discovery Inspector Components ........................................... 1-5
Advanced Threat Scan Engine ....................................................... 1-5
   True File Type ........................................................................... 1-6
   Multi-packed/Multi-layered Files ............................................. 1-6
   IntelliTrap .............................................................................. 1-6
   Network Virus Scan ............................................................. 1-7
   Content Exploit Detection .................................................... 1-7
   Network Content Inspection Engine ...................................... 1-7
   Network Content Correlation Engine .................................... 1-7
   Offline Monitoring ............................................................... 1-7

Chapter 2: Planning Deep Discovery Inspector Installation

Installation Considerations .............................................................. 2-2
Installation Scenarios ...................................................................... 2-3
   Single Port Monitoring .......................................................... 2-3
   Dual Port Monitoring ............................................................ 2-4
   Network Tap Monitoring ....................................................... 2-5
   Redundant Networks ............................................................ 2-7
Chapter 3: Installing Deep Discovery Inspector

Installation Overview ............................................................................ 3-2
System Requirements ............................................................................ 3-3
  Additional Setup Considerations ......................................................... 3-4
Installing Deep Discovery Inspector .................................................... 3-7

Chapter 4: The Preconfiguration Console

The Preconfiguration Console ................................................................. 4-2
  Preconfiguration Console Access ....................................................... 4-2
Preconfiguration Menu ........................................................................ 4-4
  Preconfiguration Menu: Device Information and Status .................... 4-6
  Preconfiguration Menu: Device Settings ........................................... 4-8
  Preconfiguration Menu: Interface Settings ....................................... 4-10
  Preconfiguration Menu: System Tasks .............................................. 4-11
  Preconfiguration Menu: View System Logs ...................................... 4-22
  Preconfiguration Menu: Change Password ..................................... 4-23
  Preconfiguration Menu: Log Off ....................................................... 4-23

Chapter 5: Getting Started

Web Console .......................................................................................... 5-2
  Web Console Password ..................................................................... 5-3
Network Settings .................................................................................. 5-4
Network Interface Settings ................................................................. 5-6
Date, Time, and Language Settings ...................................................... 5-8
Proxy Settings ..................................................................................... 5-8
Licenses and Activation Codes ............................................................ 5-9
  Activation Codes .............................................................................. 5-9
  Product Version ................................................................................ 5-9
Component Updates ................................................................. 5-11
Manual Updates ........................................................................... 5-14
Scheduled Updates ................................................................. 5-15
Update Source ............................................................................ 5-15

Chapter 6: Configuring Product Settings

Deep Discovery Inspector Notifications ........................................... 6-2
Threshold-based Notifications ....................................................... 6-2
  Notification for Threat Events ................................................ 6-3
  Notification for Detection of High Risk Hosts ....................... 6-4
  Notification for Detection of Suspicious Hosts .................... 6-5
  Notification for High Network Traffic .................................. 6-6
  Notification for File Analysis Status .................................... 6-7
Delivery Options ........................................................................ 6-7
  Email Settings .................................................................... 6-7
Network Configuration ................................................................. 6-8
  Monitored Networks ............................................................ 6-9
  Registered Domains ............................................................ 6-10
  Registered Services ............................................................... 6-11
Export/Import Configuration ....................................................... 6-12
Detection Settings ....................................................................... 6-13
  Threat Detections ............................................................... 6-13
  Application Filters ............................................................... 6-14
  Smart Protection Technology .............................................. 6-15
  Web Reputation ................................................................. 6-17
Detection Exclusion List .............................................................. 6-21
Integration with Trend Micro Products and Services ................. 6-22
Global Settings ........................................................................... 6-25
  System Settings ................................................................. 6-25
  System Time ...................................................................... 6-25
  Web Console Timeout ............................................................... 6-25
  Proxy Settings .................................................................. 6-26
Backup/Restore Appliance Configuration ................................. 6-26
Import Custom Virtual Analyzer ............................................... 6-28
System Maintenance ................................................................... 6-30
Chapter 7: Viewing and Analyzing Information

Dashboard ................................................................. 7-2
Displaying System Threat Data .................................. 7-6
Deep Discovery Inspector Custom Tabs ....................... 7-7
Using Widgets .......................................................... 7-10
  Threat Geographic Map Tab ..................................... 7-12
  Real-time Monitoring Tab ....................................... 7-14
  Virtual Analyzer Tab .............................................. 7-22
  Top Threats Tab .................................................... 7-26
  System Status Tab ................................................ 7-34
Customizing the Dashboard ....................................... 7-37

Detections ................................................................. 7-38
Detection Details ...................................................... 7-40

Logs ........................................................................... 7-55
Detection Logs Query ................................................ 7-55
Detection Log Query Details ...................................... 7-61
System Logs Query .................................................. 7-64
Syslog Server Settings ............................................. 7-65
Using Logs ............................................................... 7-65

Reports ...................................................................... 7-66
Table of Contents

Generated Reports ................................................................. 7-66
Scheduled Reports ................................................................. 7-67
On-Demand Reports ............................................................... 7-67
Report Notification Settings .................................................. 7-67
Using Reports ........................................................................... 7-68
Scheduled Reports ................................................................. 7-68
Virtual Analyzer Reports ......................................................... 7-68

Chapter 8: Maintenance

Licenses and Activation Codes ................................................... 8-2
Log/Report Maintenance ......................................................... 8-2
Appliance Rescue ...................................................................... 8-3

Chapter 9: Getting Help

Frequently Asked Questions (FAQs) .............................................. 9-2
Before Contacting Technical Support ....................................... 9-7
Trend Community ................................................................... 9-7
The Trend Micro Support Portal .............................................. 9-7
Security Information Center ..................................................... 9-7
Contacting Trend Micro .......................................................... 9-8
Technical Support .................................................................. 9-8
TrendLabs ............................................................................... 9-9
Sending Suspicious Files to Trend Micro ................................. 9-9
Documentation Feedback ........................................................ 9-10

Chapter 10: Glossary

Appendix A: Creating a Custom Virtual Analyzer

Creating a Custom Virtual Analyzer .......................................... A-1
Converting a VMware Image ..................................................... A-2
Installing Applications ............................................................ A-2
Configuring Automatic Login .................................................. A-2
Converting VMware Image with VMware Converter .................. A-3
Creating a Virtual Analyzer Image with VirtualBox ........................................A-11
Downloading and Installing VirtualBox ...........................................................A-11
Preparing the Operating System ISO .............................................................A-12
Create a new Virtual Analyzer Image ............................................................A-13
Setting up the Operating System ..................................................................A-23
Taking a Snapshot .......................................................................................A-29
Installing Applications ..................................................................................A-31
  Microsoft Office ......................................................................................A-31
  Adobe Acrobat Reader .............................................................................A-31
  .Net Framework ....................................................................................A-32
Configuring Automatic Login ......................................................................A-32
  Windows 7 .............................................................................................A-32
  Windows XP ...........................................................................................A-33
Using VirtualBox to Export an OVA Image ..................................................A-33
Using VirtualBox to Mount and Verify VMDK .............................................A-36
Uploading Virtual Machine Images to Deep Discovery Inspector and
  Configuring Virtual Analyzer ....................................................................A-43
Troubleshooting .........................................................................................A-45
Preface


This preface discusses the following topics:

- *Terminology and Documentation* on page x
- *Audience* on page xi
- *Document Conventions* on page xii
Terminology and Documentation

The following terminology is used throughout the documentation:

**TABLE P-1.** Terminology used in Deep Discovery Inspector documentation

<table>
<thead>
<tr>
<th>TERMINOLOGY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>hardware appliance</td>
<td>Deep Discovery Inspector pre-installed on a server provided by Trend Micro.</td>
</tr>
<tr>
<td>virtual appliance</td>
<td>Deep Discovery Inspector as a virtual appliance that can be installed on a bare metal server with VMware™ vSphere™ 4.x and 5.0.</td>
</tr>
</tbody>
</table>

**Note:** The term appliance is used throughout the documentation to refer to any form of Deep Discovery Inspector.

The product documentation consists of the following:

**TABLE P-2.** Deep Discovery Inspector documentation

<table>
<thead>
<tr>
<th>DOCUMENTATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator’s Guide</td>
<td>A PDF document that discusses product installation, configuration, use, and maintenance.</td>
</tr>
<tr>
<td>Help</td>
<td>HTML files compiled in WebHelp format that provide &quot;how to's&quot;, usage advice, and field-specific information. To access Help, open the web console and click the help icon.</td>
</tr>
<tr>
<td>Readme file</td>
<td>This file contains a list of what is new in the current release, basic installation steps, any known issues, and third-party license agreements. It may also contain the latest product information not found in the Help or printed documentation.</td>
</tr>
</tbody>
</table>
The Administrator’s Guide and readme file are available on the Deep Discovery Inspector Solutions CD and online:

http://docs.trendmicro.com/

**Audience**

The Deep Discovery Inspector 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 (IP address, Subnet Mask, LAN settings)
- Network devices and their administration
- Network configuration (use of VLAN, SNMP).

<table>
<thead>
<tr>
<th>DOCUMENTATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>End User License Agreement</td>
<td>The EULA contains the licensing agreement for Deep Discovery Inspector.</td>
</tr>
</tbody>
</table>
Document Conventions

To help locate and interpret information, Deep Discovery Inspector documentation uses the following conventions.

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL CAPITALS</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Menus and menu commands, command buttons, tabs, options, and tasks</td>
</tr>
<tr>
<td><em>Italics</em></td>
<td>References to other documentation or new technology components</td>
</tr>
<tr>
<td><strong>LOGS &gt; LOG MAINTENANCE</strong></td>
<td>Breadcrumbs associated with procedures to help users navigate to the relevant web console screen. Multiple breadcrumbs means that there are several ways to get to the same screen.</td>
</tr>
<tr>
<td><strong>Note:</strong> text</td>
<td>Provides configuration notes or recommendations</td>
</tr>
<tr>
<td><strong>Tip:</strong> text</td>
<td>Provides best practice information and Trend Micro recommendations</td>
</tr>
<tr>
<td><strong>WARNING!</strong> text</td>
<td>Provides warnings about activities that may harm computers on your network</td>
</tr>
</tbody>
</table>
Chapter 1

Introducing Deep Discovery Inspector

This chapter introduces product features, capabilities, and technology.

The topics discussed in this chapter are:

- *About Deep Discovery Inspector* on page 1-2
- *Deep Discovery Inspector Features* on page 1-3
- *Deep Discovery Inspector Components* on page 1-5
About Deep Discovery Inspector

Deep Discovery Inspector is a third-generation threat management solution, designed and architected by Trend Micro to deliver breakthrough APT and targeted attack visibility, insight, and control.

Deep Discovery Inspector is the result of Trend Micro’s thorough investigations of targeted attacks around the world, interviews with major customers, and the participation of a special product advisory board made up of leading G1000 organizations and government agencies.

Deep Discovery Inspector provides IT administrators with critical security information, alerts, and reports.

Threat Management Capabilities

Deep Discovery Inspector detects and identifies evasive threats in real-time, along with providing in-depth analysis and actionable intelligence needed to discover, prevent, and contain attacks against corporate data.

Expanded APT and Targeted Attack Detection

Deep Discovery Inspector detection engines deliver expanded APT and targeted attack detection including custom virtual analyzer and new discovery and correlation rules designed to detect malicious content, communication, and behavior across every stage of an attack sequence.

Visibility, Analysis, and Action

The Deep Discovery Inspector web console provides real-time threat visibility and analysis in an intuitive multi-level format that allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures.

High Capacity Platforms

Deep Discovery Inspector features are useful for a company of any size, and are vital to larger organizations needing to reduce the risk of targeted attacks. Deep Discovery Inspector features a new high-performance architecture designed to meet the demanding and diverse capacity requirements of large organizations.
Deep Discovery Inspector Features

Deep Discovery Inspector 3.2 includes the following new features:

**TABLE 1-1. Deep Discovery Inspector 3.2 Features**

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better virtual analyzer visibility</td>
<td>Deep Discovery Inspector provides the ability to view multiple logs on the virtual analyzer detection widget (the past one hour, 24 hours, 7 days, and 30 days).</td>
</tr>
<tr>
<td>Improved analysis reports</td>
<td>Deep Discovery Inspector provides detailed analysis reports, which summarize analysis results.</td>
</tr>
<tr>
<td>Improved threat detection integration</td>
<td>Deep Discovery Inspector interfaces with Threat Connect, in order to correlate known threats with detections, and provide actionable recommendations.</td>
</tr>
<tr>
<td>Asian character support</td>
<td>Deep Discovery Inspector supports the use of double-byte characters in detection logs and reports.</td>
</tr>
<tr>
<td>Deep Discovery Advisor integration</td>
<td>Deep Discovery Inspector integrates with Deep Discovery Advisor to provide more effective inspection of untrusted programs.</td>
</tr>
<tr>
<td>Custom file types</td>
<td>Virtual analyzer accepts customized files types.</td>
</tr>
<tr>
<td>Virtual analyzer results query</td>
<td>Virtual analyzer reports can be accessed from the log query page.</td>
</tr>
<tr>
<td>Virtual analysis notification</td>
<td>Deep Discovery Inspector send an email notification in the event the Virtual Analyzer is unable to analyze a file.</td>
</tr>
<tr>
<td>Report notification</td>
<td>Deep Discovery Inspector sends notification when a detailed report is available.</td>
</tr>
<tr>
<td>Improved virtual analyzer loading</td>
<td>This version allows users to browse their local file system from a uploader tool, without accessing an FTP or HTTP server.</td>
</tr>
</tbody>
</table>
The Virus Scan Engine has been upgraded to an Advanced Threat Scan Engine.

Virtual analysis results have been added to reports.

Two new columns have been added: "Correlation Incident" and "Virtual Analysis Detections". An additional time frame has been added: "Past 1 hour". Response time has been enhanced to within 5 seconds.

Users can input their own SSL certificate.

Users can now use the "Ping" command (in the Pre-configuration menu) to test the network configuration.

Virtual Analyzer widget added to display virtual analysis results.

Users can select various activations codes based on business needs.

Users can view the maximum bandwidth capacity.

Users can select a CEF or LEEF syslog format.

An enlarged disk partition supports the increase in pattern/engine size.

A network traffic indicator is available on all screens.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgraded Virus Scan Engine</td>
<td>The Virus Scan Engine has been upgraded to an Advanced Threat Scan Engine.</td>
</tr>
<tr>
<td>Enhanced report</td>
<td>Virtual analysis results have been added to reports.</td>
</tr>
<tr>
<td>Detections page enhancements</td>
<td>Two new columns have been added: &quot;Correlation Incident&quot; and &quot;Virtual Analysis Detections&quot;. An additional time frame has been added: &quot;Past 1 hour&quot;. Response time has been enhanced to within 5 seconds.</td>
</tr>
<tr>
<td>Import certificate</td>
<td>Users can input their own SSL certificate.</td>
</tr>
<tr>
<td>Troubleshooting tool on the Command Line Interface</td>
<td>Users can now use the &quot;Ping&quot; command (in the Pre-configuration menu) to test the network configuration.</td>
</tr>
<tr>
<td>New widget</td>
<td>Virtual Analyzer widget added to display virtual analysis results.</td>
</tr>
<tr>
<td>Additional Activation Codes</td>
<td>Users can select various activations codes based on business needs.</td>
</tr>
<tr>
<td>Additional information on the Product License page</td>
<td>Users can view the maximum bandwidth capacity.</td>
</tr>
<tr>
<td>Additional syslog options</td>
<td>Users can select a CEF or LEEF syslog format.</td>
</tr>
<tr>
<td>Enhanced engine/pattern storage</td>
<td>An enlarged disk partition supports the increase in pattern/engine size.</td>
</tr>
<tr>
<td>Additional information bars</td>
<td>A network traffic indicator is available on all screens.</td>
</tr>
</tbody>
</table>
Introducing Deep Discovery Inspector

Note:
For a complete list of Trend Micro products and services that integrate with Deep Discovery Inspector, see Integration with Trend Micro Products and Services on page 6-22.

Deep Discovery Inspector Components

Deep Discovery Inspector uses the mirror port of a switch to monitor network traffic and detect known and potential security risks. Deep Discovery Inspector components include:

Advanced Threat Scan Engine

The Advanced Threat Scan Engine is an upgrade from the standard virus scan engine. ATSE uses a combination of a file-based detection-scanning and heuristic rule-based scanning in order to provide better detection of system vulnerabilities.

The virus scan engine uses the virus pattern file to analyze files traveling on your network. To ensure that your appliance is using the latest pattern file, regularly update Deep Discovery Inspector (see Component Updates on page 5-11).

The virus scan engine uses the following methods of detection:

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

TABLE 1-1. Deep Discovery Inspector 3.2 Features (Continued)

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated Threat Geographic Map</td>
<td>User can easily select a default location.</td>
</tr>
<tr>
<td>Deep Correlation log query update</td>
<td>Users can query the Deep Correlation log and view results on the log query page.</td>
</tr>
<tr>
<td>Additional known good file look up capability</td>
<td>Users can enable/disable a GRID lookup on a file, prior to submitting it to the Virtual Analyzer.</td>
</tr>
</tbody>
</table>

Deep Discovery Inspector Components

Deep Discovery Inspector uses the mirror port of a switch to monitor network traffic and detect known and potential security risks. Deep Discovery Inspector components include:

Advanced Threat Scan Engine

The Advanced Threat Scan Engine is an upgrade from the standard virus scan engine. ATSE uses a combination of a file-based detection-scanning and heuristic rule-based scanning in order to provide better detection of system vulnerabilities.

The virus scan engine uses the virus pattern file to analyze files traveling on your network. To ensure that your appliance is using the latest pattern file, regularly update Deep Discovery Inspector (see Component Updates on page 5-11).

The virus scan engine uses the following methods of detection:

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

TABLE 1-1. Deep Discovery Inspector 3.2 Features (Continued)

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated Threat Geographic Map</td>
<td>User can easily select a default location.</td>
</tr>
<tr>
<td>Deep Correlation log query update</td>
<td>Users can query the Deep Correlation log and view results on the log query page.</td>
</tr>
<tr>
<td>Additional known good file look up capability</td>
<td>Users can enable/disable a GRID lookup on a file, prior to submitting it to the Virtual Analyzer.</td>
</tr>
</tbody>
</table>

Note: For a complete list of Trend Micro products and services that integrate with Deep Discovery Inspector, see Integration with Trend Micro Products and Services on page 6-22.
True File Type

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

With true file type, Deep Discovery Inspector determines a file’s true type and skips inert file types, 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 Deep Discovery Inspector evaluate compressed files that could contain viruses or other Internet threats.

The Advanced Threat Scan Engine uses the following methods of detection:
- Network Virus Scan
- Content Exploit Detection
- Network Content Inspection Engine
- Network Content Correlation Engine
Network Virus Scan
Deep Discovery Inspector uses a combination of patterns and heuristics to proactively detect network viruses. The product monitors network packets and trigger events that can indicate an attack against a network. The product can also scan traffic in specific network segments.

Content Exploit Detection
Deep Discovery Inspector uses heuristics technology to verify whether the content of various commonly used file types contain suspicious shell code or vulnerabilities.

Network Content Inspection Engine
Network Content Inspection Engine is the program module used by Deep Discovery Inspector to scans content passing through the network layer.

Network Content Correlation Engine
Network Content Correlation Engine is the program module used by Deep Discovery Inspector 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 Correlation Engine categorizes as an executable or potentially malicious file. 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. Deep Discovery Inspector captures potential risk files, enters a log in the database, and saves a copy of the file, which can be uploaded to the Virtual Analyzer for further analysis. The file session and threat information are captured as a file header and stored in the log file.

Offline Monitoring
Deep Discovery Inspector deploys in offline mode. It monitors network traffic by connecting to the mirror port on a switch for minimal or no network interruption.
Multiple Protocol Support

Deep Discovery Inspector monitors network activities including those that use the HTTP, FTP, SMTP, SNMP, and P2P protocols.
Planning Deep Discovery Inspector
Installation

This chapter provides tips, suggestions, and requirements for installing Deep Discovery Inspector.

The topics discussed in this chapter are:

- Installation Considerations on page 2-2
- Installation Scenarios on page 2-3
Installation Considerations

Consider the following before installing Deep Discovery Inspector.

- Port speeds must match.

  The destination port speed should be the same as the source port speed to ensure equal port mirroring. 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.

  For Virtual Analyzer additional considerations apply:
  - Isolate Network: does not exchange data with Internet.
  - Specified Network: uses a specified data port to exchange data with Internet.
  - Management Network: uses a management port to exchange data with Internet.

- Specified network needs one more data port.

**Tip:** For better performance, when installing Deep Discovery Inspector it is recommended to use a plug-in NIC (rather than an onboard NIC) as a data port.

- The appliance monitors the complete data flow.

  Deep Discovery Inspector monitors all data coming into and going out of the network.
Installation Scenarios

Use the following examples to plan a customized Deep Discovery Inspector installation.

Single Port Monitoring

The Deep Discovery Inspector data port is connected to the mirror port of the core switch, which mirrors the port to the firewall.

![Diagram of Single Port Monitoring setup](image)

**Figure 2-2.** Single Port Monitoring
Dual Port Monitoring

Deep Discovery Inspector can monitor different network segments using different data ports. Deep Discovery Inspector data ports are connected to the mirror ports of access or distribution switches.

FIGURE 2-3. Dual Port Monitoring
Network Tap Monitoring

Network taps monitor the data flowing across the network from interconnected switches, routers, and computers. Multiple Deep Discovery Inspector appliances can be connected to a network tap.

**Note:** If using network taps, ensure that they copy DHCP traffic to Deep Discovery Inspector instead of filtering DHCP traffic.

![Diagram](image)

**Figure 2-4.** Single Deep Discovery Inspector Device connected to a Network Tap
Additionally, use an Intrusion Detection System (IDS) load balancer for better performance when deploying multiple Deep Discovery Inspector appliances.

**FIGURE 2-5.** Multiple Deep Discovery Inspector Appliances connected to a Network Tap
Redundant Networks

Many enterprise environments use redundant networks to provide high availability. When an asymmetric route is available, connect Deep Discovery Inspector to redundant switches.

![Figure 2-6. Redundant Network Monitoring](image)

Specific VLANs

Some enterprise environments limit port scanning to specific VLANs in order to optimize bandwidth and resource use. In this scenario, connect Deep Discovery Inspector to a switch if the mirror configuration is VLAN-based.
Remote Port or VLAN Mirroring

Use remote mirroring when:

- Monitoring switches
- Local switches do not have enough physical ports
- Port speed on local switches do not match (GB versus MB).

**FIGURE 2-7. Remote Port or VLAN Mirroring**
Mirroring Trunk Links

When there are multiple encapsulated VLANs in the same physical link, mirror the source port from a trunk link. Ensure that the switch mirrors the correct VLAN tag to Deep Discovery Inspector for both directions.

![Mirroring Trunk Links Diagram](image)

**FIGURE 2-8. Mirroring Trunk Links**
Chapter 3

Installing Deep Discovery Inspector

This chapter details the steps for installing the software.

The topics discussed in this chapter are as follows:

- Installation Overview on page 3-2
- System Requirements on page 3-3
- Installing Deep Discovery Inspector on page 3-7
Installation Overview

This Deep Discovery Inspector version is available in several form factors:

<table>
<thead>
<tr>
<th>hardware appliance</th>
<th>Deep Discovery Inspector pre-installed on a server provided by Trend Micro.</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual appliance</td>
<td>Deep Discovery Inspector as a virtual appliance that can be installed on a bare metal server with VMware™ vSphere™ 4.x and 5.0.</td>
</tr>
</tbody>
</table>

Deep Discovery Inspector only supports fresh installations. Users who have previously set up a threat discovery device or virtual appliance can upgrade to this version by performing a fresh installation. For details, see Backup/Restore Appliance Configuration on page 6-26.

**Note:** Configuration files from previous appliance versions cannot be used in this version.

The software is packaged as an ISO file, and installed on a purpose-built, hardened, performance-tuned 64-bit Linux operating system, included in the package.

Install the software on a bare metal server that meets the requirements listed in System Requirements on page 3-3. The bare metal installation boots from the Deep Discovery Inspector installation CD (which contains the ISO file) to begin the process.

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

Deep Discovery Inspector requires the following:

**TABLE 3-1. System requirements**

<table>
<thead>
<tr>
<th>RESOURCES</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
</table>
| Host machine    | • **CPU**: Two Intel™ Core™2 Quad processors recommended  
|                 | • **RAM**: 8GB minimum  
|                 | • **Hard disk space**: 100GB minimum  
|                 | **Note**: For additional log storage space, 300-500GB is recommended.  
|                 | • **Network interface card (NIC)**: Two NICs minimum  
|                 | **Note**: For better performance, when installing Deep Discovery Inspector, use a plug-in NIC (rather than an onboard NIC) as a data port.  
| ESXi server     | 4.x or 5.0                                                                   |
### TABLE 3-1. System requirements

<table>
<thead>
<tr>
<th>RESOURCES</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
</table>
| Preconfiguration console  | Access to the Preconfiguration console requires the following:  
  **For VGA connection:**  
  • Monitor with a VGA port  
  • VGA cable  
  **For SSH connection:**  
  • Computer with an Ethernet port  
  • General Ethernet cable  
  • SSH communication application (PuTTY, or another terminal emulator)  
  **For serial connection:**  
  • Computer with a serial port  
  • RS232 serial cable  
  • Serial communication application (HyperTerminal) |
| Web Console                | Access to the web console requires any of the following browsers:  
  • Microsoft Internet™ Explorer™ 8.0 or 9.0  
  • Mozilla™ FireFox™ 4.x, 5.x, or higher  
  • Adobe Flash player 8.0 or higher |

### Additional Setup Considerations

Set these options to enable Deep Discovery Inspector web console navigation.
To set Security options for Internet Explorer:

Note: For all IE versions, ensure that the following options are enabled.

1. On the browser, go to Tools > Internet Options > Security tab.
2. Select the Internet zone and click Custom level....
3. On the Miscellaneous section > Allow META REFRESH, select Enable > OK.
4. Repeat steps 1-3 for Local intranet and Trusted sites zones.
5. Verify that browser zoom is set to 100%.

To set JavaScript options for Internet Explorer:

1. On your browser, go to Tools > Internet Options > Security tab.
2. Select the Internet zone and click Custom level...
3. On the Scripting section > check Enable active Scripting > OK.

To set JavaScript options for Firefox:

1. On your browser, go to Tools > Options > Content tab.
2. Check Enable JavaScript > OK.

To set options for a virtual appliance deploying in ESXi 4.X or 5.0:

1. On the vSphere Client >Inventory page, right-click the appliance name and select Edit Settings...
   The settings screen appears.
2. On the settings screen, click the Options tab and select VMware Tools.
3. Uncheck Synchronize guest time with host to disable this option.
FIGURE 3-1. Virtual Appliance Options
Installing Deep Discovery Inspector

This topic discusses how to install Deep Discovery Inspector on a bare metal server.

To install Deep Discovery Inspector on a bare metal server:

1. Connect a monitor to Deep Discovery Inspector through a VGA port.
2. Insert the Deep Discovery Inspector installation CD into the CD/DVD drive.
3. Power on the bare metal server.
   The BIOS Boot Manager screen appears.

   ![BIOS Boot Manager Screen](image)

4. At the BIOS Boot Manager screen, press F11.

   **Note:** When installing Deep Discovery Inspector through a serial connection, press ESC following by "1" (Shift + 1) to enter BIOS Boot Manager.

   The Boot Manager screen appears.
5. At the Boot Manager screen, select SATA Optical Drive and press ENTER. The Deep Discovery Inspector Installation screen appears.

Note: When installing Deep Discovery Inspector through a serial connection, type "serial" and press ENTER.

---

**FIGURE 3-5. System Information Screen**

7. At the system information screen, perform the following steps:
   a. By default, the installer performs a system requirements check before installing Deep Discovery to confirm that the host machine has the necessary resources to run the product. If the purpose of installation is to test the product in a controlled environment before installing it on your network, type 2 and press ENTER to skip the system requirements check.
   b. To obtain installation logs (used for troubleshooting installation problems) type 3 and press ENTER.
   c. Type 1 and press ENTER to begin the installation.

The Management Port screen appears.
8. At the Management Port Selection screen:
   a. Verify that the network port status and the actual port status match. If there is a status conflict, select **Re-detect** and press **ENTER** to refresh the status.
   b. To determine which active link card is connected to the management domain, perform the steps indicated on the Management Port Selection screen.
   c. Select an active link card and press **ENTER**.
      Installation continues and completes.

9. If installation log collection was enabled in step 7b a list of storage devices is displayed on the Export Installation Logs screen. Perform the following steps:
FIGURE 3-7. Export Installation Logs Screen

a. Select a device to which to save the logs and press ENTER. When the installation log file name appears, press ENTER.

**Note:** The recommended device to save the logs to is sda11.

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

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

The system automatically restarts and the Preconfiguration Console appears.
The installation CD (if used) is ejected from the CD/DVD drive.

c. Remove the CD to prevent reinstallation.

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

**Note:** All listed steps are identical for both hardware and virtual form factors.
The Preconfiguration Console

This chapter explains how to use the Preconfiguration console to perform initial Deep Discovery Inspector configuration, and some maintenance tasks.

The topics discussed in this chapter are:

- *The Preconfiguration Console* on page 4-2
- *Preconfiguration Console Access* on page 4-2
- *Preconfiguration Menu* on page 4-4
- *Preconfiguration Menu: Device Information and Status* on page 4-6
- *Preconfiguration Menu: Device Settings* on page 4-8
- *Preconfiguration Menu: Interface Settings* on page 4-10
- *Preconfiguration Menu: System Tasks* on page 4-11
- *Preconfiguration Menu: View System Logs* on page 4-22
- *Preconfiguration Menu: Change Password* on page 4-23
- *Preconfiguration Menu: Log Off* on page 4-23
The Preconfiguration Console

The Preconfiguration Console is a terminal communications program that enables configuring or viewing of any preconfiguration settings including:

- Network settings
- System

Use the Preconfiguration Console to:

- Configure initial settings (product IP address and host name)
- Roll back any updates
- Import/export device configuration
- Import HTTPS certificates
- Ping the network to verify configuration
- Perform a diagnostic test
- Restart the device
- View the system logs

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

Preconfiguration Console Access

This topic discusses how to access the Preconfiguration Console.

To access the Preconfiguration Console:

1. Select one of the following methods to access the Preconfiguration Console.

   - From a monitor with a VGA port (recommended):
     Connect the monitor VGA port to the software appliance VGA port using a VGA cable.

   - From a computer with an Ethernet port:
     a. Connect the computer's Ethernet port to the management port of the software appliance using an Ethernet cable.
b. On the computer, open an SSH communication application (PuTTY, or another terminal emulator).

**Note:** An SSH must be enabled to use PuTTY, or another terminal emulator. See *To enable/disable an SSH connection:* on page 6-30.

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

c. Use the following values when accessing the console for the first time:
   - IP address (for SSH connection only): the default is 192.168.252.1
   - User name: admin
   - Password: press ENTER
   - Port number: 22

**From a computer with a serial port:**

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

b. On the computer, open a serial communication application (HyperTerminal).

c. Use the following values if you are accessing the console for the first time:
   - Bits per second: 115200
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
2. When the Preconfiguration Console screen opens, type the default password admin and press ENTER twice.

![Logon Screen](image1)

**FIGURE 4-1. Logon Screen**

**Preconfiguration Menu**

![Preconfiguration Console Main Menu](image2)

**FIGURE 4-2. Preconfiguration Console Main Menu**
The Preconfiguration Console menu displays the following:

**TABLE 4-1. Main menu item descriptions**

<table>
<thead>
<tr>
<th>MENU ITEMS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information and Status</td>
<td>View product information and monitor memory usage.</td>
</tr>
<tr>
<td>Device Settings</td>
<td>Modify the product’s host name, IP address, subnet mask, and the network default gateway address and DNS servers. Register Deep Discovery Inspector to Trend Micro Control Manager for centralized management.</td>
</tr>
<tr>
<td>Interface Settings</td>
<td>View the network speed and duplex mode for the management port, which Deep Discovery Inspector automatically detects.</td>
</tr>
<tr>
<td>System Tasks</td>
<td>Roll back to the previous update, perform a diagnostic test, or restart the product. You can also import or export the configuration file and import the HTTPS certificate. It is also possible to ping a server in the same subnet.</td>
</tr>
<tr>
<td>View System Logs</td>
<td>View logs detailing security risks and events.</td>
</tr>
<tr>
<td>Change Password</td>
<td>Change the root password.</td>
</tr>
<tr>
<td>Log Off with Saving</td>
<td>Log off from the Preconfiguration Console after saving the changes.</td>
</tr>
<tr>
<td>Log Off without Saving</td>
<td>Log off from the Preconfiguration Console without saving the changes.</td>
</tr>
</tbody>
</table>

To access a menu item, type the number for the menu item and then press ENTER.
Preconfiguration Menu: Device Information and Status

View the product name, program version, and memory usage on this screen. Memory usage information can also be viewed on the Deep Discovery Inspector’s web console: Dashboard > System Status tab. For details, see Detections on page 7-38.

To view product information:

1. Log on to the Preconfiguration Console.

   The Main Menu appears.

   ![Preconfiguration Console Main Menu](image)

   **FIGURE 4-3.** Preconfiguration Console Main Menu
2. Type 1 to select **Device Information & Status** and press ENTER.
   The Device Information and Status screen appears.

   ![Device Information and Status Screen](image)

   **FIGURE 4-4.** Device Information and Status Screen

3. Press ENTER to return to the main menu.
Preconfiguration Menu: Device Settings

---

**Management IP Address Settings**
- **Type:** [Static] (Use Space to change the value)
- **IP address:** 192.168.255.1
- **Subnet mask:** 255.255.255.0
- **Gateway:** 192.168.255.254
- **DNS server 1:**
- **DNS server 2:**
- **Host name:** localhost

**Bind IP address**
- **UI/AM IP:**

**Register to Trend Micro Control Manager:** [No]
- **FQDN or IP address:**
- **Enable two-way communication port forwarding:** [No]
- **Port forwarding IP address:**
- **Port forwarding port number:**

**Return to main menu**
- **Press Enter to leave without saving.**

---

**FIGURE 4-5. Device Settings Screen**

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

---

**Note:** These tasks can also be performed on the web console.

---

**To modify settings using the Preconfiguration Console:**

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

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

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

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

4. Type a new host name.

5. (Optional) Type a VLAN ID.

6. (Optional) Register to Trend Micro Control Manager.

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

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

   b. Type the Control Manager IP address.

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

   d. To enable two-way communication between Deep Discovery Inspector and Trend Micro Control Manager, type the IP address and port number of your router or NAT device in the Port forwarding IP address and Port forwarding port number fields.

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

7. Navigate to Return to main menu and press ENTER to return to the main menu.

8. Type 7 and press ENTER to save the settings.
Preconfiguration Menu: Interface Settings

By default, Deep Discovery Inspector automatically detects the network speed and duplex mode for the management port (MGMT); it is unlikely these settings need to be changed. However, if any connection issues occur, manually configure these settings.

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

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

Note: Data ports used by Deep Discovery Inspector can be managed from the web console: Administration > Global Settings > Network Interface Settings. For details, see Network Interface Settings on page 5-6.
To modify interface settings:

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

Preconfiguration Menu: System Tasks

Use the System Tasks screen if an error message requires any of the following:

• a Deep Discovery Inspector update roll back
• a configuration file import or export
• an HTTPS certificate import
• a diagnostic test to test the network configuration
• a ping test to verify network configuration
• a Deep Discovery Inspector restart.

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

Perform the following tasks:

• Rolling back to the Previous Update on page 4-12
• Importing the Configuration File (HyperTerminal only) on page 4-13
• Exporting the Configuration File (HyperTerminal only) on page 4-16
• Importing the HTTPS Certificate (HyperTerminal only) on page 4-18
• Performing a Diagnostic Test on page 4-19
• Performing a Ping Test on page 4-19
• Restarting Deep Discovery Inspector on page 4-20

Rolling back to the Previous Update
If an update causes operational problems or is not compatible with Deep Discovery Inspector, roll back to the previous update.

To roll back to the previous update:
1. Log on to the Preconfiguration Console.
   The Main Menu appears.
2. Type 4 and press ENTER.
   The System Tasks screen appears.

![System Tasks Screen](image)

**FIGURE 4-7. System Tasks Screen**
3. Type 1 and press ENTER.
   The Rollback to previous update screen appears.

   **Note:** Rolling back to a previous update may require restarting Deep Discovery Inspector.

![Rollback to Previous Update Screen](image)

4. Select **OK** and press ENTER.
   The product rolls back to the previous updates.

5. Type 7 and press ENTER to return to the main menu.

**Importing the Configuration File (HyperTerminal only)**

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

**WARNING!** Export the current configuration settings before importing the backup configuration file. For details, see *Exporting the Configuration File (HyperTerminal only)* on page 4-16.
To import the backup configuration file:

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

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

5. Browse to the configuration file to be imported.
6. Change the protocol to Kermit and click Send.

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

The device imports the configuration file and uses the settings from the file.
Exporting the Configuration File (HyperTerminal only)

Regularly back up the configuration files to ensure the latest configuration settings are used.

To export the configuration file:

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

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

**FIGURE 4-12. Preconfiguration Console Receive File Screen**
5. Browse to the configuration file to be exported.

![Receive File Screen](image)

**FIGURE 4-13. Receive File Screen**

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

   The device exports the configuration settings to a config.dat file.

![Kermit File Receive Screen](image)

**FIGURE 4-14. Kermit File Receive Screen**

7. Rename the exported configuration files to keep track of the latest configuration files.
Importing the HTTPS Certificate (HyperTerminal only)

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

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

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

To import the HTTPS certificate:

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

---
To import the HTTPS certificate using HyperTerminal:
1. Click Transfer > Send File.
2. Browse the certificate file that you want to import, select the Protocol to Kermit, and then click Send.
   Press <CTRL+C> three times to cancel importing.

**Import the HTTPS certificate now?**

- [OK] OK
- [Cancel] Cancel

---

**FIGURE 4-15. Import HTTPS Certificate Screen**

4. From the HyperTerminal menu, click Transfer > Send File.
5. Browse to the HTTPS certificate file to be imported.
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, in order to identify any software issues.

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

Performing a Ping Test
Use this feature to verify network configuration.

To perform the "ping" test:
1. Log on to the Preconfiguration Console.
   The Main Menu appears.
2. Type 4 and press ENTER.
   The System Tasks screen appears.
3. Type 7 and press ENTER.
   The Ping Test screen appears.
4. Input the server IP address and press PING.
   Ping test results appear on-screen.
5. Press ESC to return to the main menu.
**Restarting Deep Discovery Inspector**

To restart Deep Discovery Inspector, access the Preconfiguration Console using a serial communication application (HyperTerminal) or an SSH utility (Deep Discovery Inspector). Using Deep Discovery Inspector to access the Preconfiguration Console enables a the device to be restarted remotely.

When Deep Discovery Inspector starts, it verifies the integrity of its configuration files. The web console password may reset itself if the configuration file containing password information is corrupted. If console log in fails, when using the preferred password, log on using the default password `admin`.
To restart Deep Discovery Inspector:

1. Log on to the Preconfiguration Console.
   The Main Menu appears.
2. Type 4 and press ENTER.
   The System Tasks screen appears.
3. Type 6 and press ENTER.
   The Reset Device screen appears.

```
Reset Trend Micro Deep Discovery Inspector and keep current configuration.

OK    Cancel
```

**FIGURE 4-16. Reset Device Screen**

Deep Discovery Inspector restarts.
Preconfiguration Menu: View System Logs

Figure 4-17. Sample System Log

The log format in the Preconfiguration Console displays the system logs. For more detailed and configurable, use the Detection Log Query on the web console. See Detection Logs Query on page 7-55.

To view system logs in the Preconfiguration Console:

1. Log on to the Preconfiguration Console.
   
   The Main Menu appears.

2. Type 5 and press ENTER.
   
   The System log screen appears.

   **Note:** Although a blank screen appears initially, logs will appear as soon as Deep Discovery Inspector detects network activity.
Preconfiguration Menu: Change Password

Change the Deep Discovery Inspector password using the Preconfiguration Console.

To change the root password in the Preconfiguration Console:

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

Preconfiguration Menu: Log Off

When logging off from the Preconfiguration Console, select one of the following:

- Log off with Saving
- Log off without Saving
To Log Off with Saving:

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

1. After making changes to the configuration settings, return to the main menu.
2. Type 7 and press ENTER.
   The Leave Preconfiguration with Saving screen appears.

3. Under Save configuration settings and exit?, navigate to OK and press ENTER.
Log Off without Saving:

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

   ![Leave Preconfiguration without Saving Screen](image)

   **FIGURE 4-20. Leave Preconfiguration without Saving Screen**

3. Under Exit without saving configuration settings?, navigate to OK and press ENTER.
Getting Started

This chapter introduces the Deep Discovery Inspector web console and basic appliance settings.

The topics discussed in this chapter are:

- Web Console on page 5-2
- Network Settings on page 5-4
- Network Interface Settings on page 5-6
- Date, Time, and Language Settings on page 5-8
- Proxy Settings on page 5-8
- Licenses and Activation Codes on page 5-9
- Component Updates on page 5-11
Web Console

Deep Discovery Inspector provides a built-in web console through which users can view system status, configure threat detection, configure and view logs, run reports, administer Deep Discovery Inspector, and obtain help. The web console includes six tabs:

- Dashboard - See Dashboard on page 7-2
- Detections - See Detections on page 7-38
- Logs - See Logs on page 7-55
- Reports - See Reports on page 7-66
- Administration - See Global Settings on page 6-25
- Help

![Deep Discovery Inspector Web Console](image)

**FIGURE 5-1. Deep Discovery Inspector Web Console**

To open the web console:

1. From a network workstation, open a browser window.

**Note:** The following browsers and versions are supported: Microsoft™ Internet Explorer™ 8.0 or 9.0 and Mozilla™ Firefox™ 4.x, 5.x., or higher.
Note: Adobe Flash player 8.0 or higher is also required.

2. Set the Internet Security level to Medium and enable ActiveX Binary and Script Behaviors, to ensure that tool tips and reports appear.

3. Using the managed port IP address set for the product during initial configuration, type the following URL exactly as it appears:

Note: The URL is case sensitive.

4. Type the default password: admin

Note: Change the password immediately after logging on for the first time. See Web Console Password on page 5-3.

5. Click Login.

Note: After changing Deep Discovery Inspector’s IP address, update browser bookmarks to reflect the new IP address.

6. Set system time. Go to Date, Time, and Language Settings on page 5-8.

7. Activate Deep Discovery Inspector to begin using it. Go to To activate or renew a license: on page 5-10.

Web Console Password

The default web console password is admin. For added security, Trend Micro recommends changing the Deep Discovery Inspector password after logging on for the first time, and periodically thereafter.

Passwords should be a combination of alphanumeric characters (0-9, a-z, A-Z, !$%^) and must be 4 to 32 characters long.

Observe these guidelines for creating a strong password:
• Avoid words found in the dictionary.
• Intentionally misspell words.
• Use phrases or combine words.
• Use both uppercase and lowercase letters.

Note: Lost passwords cannot be recovered. Contact your support provider for assistance in resetting the password.

To change the Deep Discovery Inspector web console password:
PATH: ADMINISTRATION > CHANGE PASSWORD
1. Type the current (old) password.
2. Type the new password and confirm it.
3. Click Save.

Network Settings

The following format rules apply to Deep Discovery Inspector network settings.

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

Appliance Host Name Format
Use the Fully Qualified Domain Name (FQDN) for the host name.
Example:
hostname.domain-1.com

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

Dynamic IP Address
Select a dynamic IP address to enable a DHCP server on your network. Verify that the preconfiguration console has been changed accordingly. See Preconfiguration Menu: Device Settings on page 4-8.
**Static IP Address Format**

IP addresses must be in the format: \texttt{XXX.XXX.XXX.XXX}, where x is a decimal value between 0 and 255.

The IP address cannot be in any of the following formats:

- \texttt{AAA.XXX.XXX.XXX}, where A is in the range 223 to 240 [Multicast Address]
- \texttt{0.0.0.0} [Local Host name]
- \texttt{255.255.255.255} [Broadcast Address]
- \texttt{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.

Example:

For \texttt{255.255.255.0}, the binary format is \texttt{11111111.11111111.11111111.00000000}.

For \texttt{255.255.252.0}, the binary format is \texttt{11111111.11111111.11111000.00000000}.

**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.
Network Interface Settings

The Network Interface Settings screen enables management of the appliance’s IP address and network interface ports.

Deep Discovery Inspector requires its own IP address to ensure that the management port can access the web console. To enable a DHCP server on your network to dynamically assign an IP address to Deep Discovery Inspector, select Dynamic IP address (DHCP). Otherwise, select static IP address.

Deep Discovery Inspector uses a management port and several data ports. To view the status of these ports, change the network speed/duplex mode for each of the data ports, and capture packets for debugging and troubleshooting purposes, go to the Appliance IP Settings screen.

Note: The network speed/duplex mode for the management port can only be configured from the Preconfiguration Console. For details, see Preconfiguration Menu: Interface Settings on page 4-10.

To configure a dynamic IP address:

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

1. In Appliance hostname, specify the host name.
2. Select Dynamic IP address (DHCP).
3. Click Save.

To configure a static IP address:

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

1. In Appliance hostname, specify the host name.
2. Select Static IP address.
3. Type the following:
   - **IP address**: The numeric address specifically for Deep Discovery Inspector
   - **Subnet Mask**: Indicates the subnet mask for the network to which the Deep Discovery Inspector IP address belongs
   - **Gateway** (optional): The IP address of the network gateway
DNS Server 1 (optional) The IP address of the primary server that resolves host names to an IP address

DNS Server 2 (optional) The IP address of the secondary server that resolves host names to an IP address

4. Click Save.

To manage network interface ports:

Path: Administration > Global Settings > Network Interface Settings > Appliance IP Settings

1. View the status for each port.
2. To change the port’s network speed and duplex mode, select from the Connection Type options.
3. Select Check VLAN tags if VLAN tags are used to differentiate TCP connections.
4. To capture packets on each port, click Start to begin packet capture.

   The date/time of the packet capture session displays next to the button. The total amount of packets captured dynamically displays on the lower section of the screen.

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

5. Click Stop when the packet capture session is done.

   **Note:** The maximum size for files containing packet data is 30MB.

6. Click View to view data for the particular packet capture session.
7. Click Export to export the data to a log file; specify the target location of the log file tcpdump.tgz.

   **Tip:** Send the log file to Trend Micro for troubleshooting assistance.

8. Click Reset to remove files containing packet data.
Date, Time, and Language Settings

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

To set the system time and language settings:

Path: Administration > Global Settings > System Settings > Date, Time, and Language

1. In Date, Time, and Language Settings, select one of the following:
   a. Synchronize appliance time with an NTP server:
      i. In NTP server, type the NTP server address.
      ii. Click Synchronize Now.
   b. Set system time manually:
      i. Select the month, day, and year using the mm/dd/yyyy format.
      ii. Select the hour, minute, and second.
2. Using the Time Zone drop down menu select the appropriate time zone.
3. Using the Language Settings drop down menu select a language to display the logs and reports in.
4. Click Save.

Proxy Settings

Deep Discovery Inspector uses the proxy settings configured in the web console when:
• Downloading updates from the Trend Micro ActiveUpdate server or another update source
• Updating the product license
• Connecting to other Trend Micro products (TMSP, Smart Protection Server, and Trend Micro Control Manager).

To configure proxy settings:

Path: Administration > Global Settings > System Settings > Proxy Settings

1. Select Use a proxy server for pattern, engine, and license updates.
2. Select HTTP, SOCKS4, or SOCKS5 for the Proxy protocol.
3. Type the **Server name** or **IP address** and the **Port** number.

4. If the proxy server requires authentication, type the **User name** and **Password** under **Proxy server authentication**.

5. Click **Test Connection** to verify connection settings.

6. Click **Save** if connection was successful.

### Licenses and Activation Codes

The Product License screen displays license information and accepts valid Activation Codes for Deep Discovery Inspector.

#### Activation Codes

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

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

If you received a **Registration Key** instead of an Activation Code, use it to register Deep Discovery Inspector at:

[https://olr.trendmicro.com/registration/](https://olr.trendmicro.com/registration/)

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

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

After registration, an Activation Code is sent via email.

### Product Version

The Activation Code sent by Trend Micro is associated with the product version.

- **Evaluation version**: Includes all the product features. Upgrade an evaluation version to the fully licensed version at any time.

- **Fully licensed version**: Includes all the product features and technical support. A 30-day grace period takes effect after the license expires. Renew the license before it expires by purchasing a maintenance renewal.
License status is displayed on the Product License screen. If you are renewing a license and need renewal instructions, click **View renewal instructions**.

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

For an evaluation version, a reminder displays when the license expires. The consequences of not upgrading to the fully licensed version are listed in **Table 5-1**.

For a fully licensed version, a reminder displays:

- 60 days before expiration ends
- 30 days before grace period ends
- When the license expires and grace period elapses. The result of not renewing the license are listed in **Table 5-1**.

**TABLE 5-1. Results of an expired Deep Discovery Inspector license**

<table>
<thead>
<tr>
<th>LICENCE TYPE AND STATUS</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation (Expired)</td>
<td>Deep Discovery Inspector disables component updates, scanning, and log transmission to TMSP. Certain on-screen information is not available. For details, see <strong>Licenses and Activation Codes</strong> on page 8-2.</td>
</tr>
<tr>
<td>Fully Licensed (Expired)</td>
<td>Technical support and component updates are not available. Deep Discovery Inspector monitors the network using out-of-date components. These components may not completely protect the network from the latest security risks.</td>
</tr>
</tbody>
</table>

**To activate or renew a license:**

**PATH:** Administration > Product License

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

**Note:** After Deep Discovery Inspector is activated, the Setup Guide is displayed. Follow the steps in the Setup Guide.

4. From the Product License Details screen, click **Update Information** to refresh the screen with the new license details.

**Note:** This screen also provides a link to your detailed license available on the Trend Micro website.

### Component Updates

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

#### Components to Update

To help protect your network, Deep Discovery Inspector uses the components listed in Table 5-2.

**TABLE 5-2. Deep Discovery Inspector Components**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Threat Scan Engine</td>
<td>ATSE checks files for less conventional threats, including document exploits. Some detected files may be safe and should be further observed and analyzed in a virtual environment.</td>
</tr>
<tr>
<td>Virus Pattern</td>
<td>Used for identifying virus signatures—unique patterns of bits and bytes that signal the presence of a virus.</td>
</tr>
</tbody>
</table>
### TABLE 5-2. Deep Discovery Inspector Components (Continued)

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware Active-monitoring Pattern</td>
<td>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.</td>
</tr>
<tr>
<td>IntelliTrap Pattern</td>
<td>Used for identifying real-time compressed executable file types that commonly hide viruses and other potential threats.</td>
</tr>
<tr>
<td>IntelliTrap Exception Pattern</td>
<td>Provides a list of real-time compressed executable file types that are commonly safe from viruses and other potential threats.</td>
</tr>
<tr>
<td>Network Content Inspection Engine</td>
<td>The engine used to perform network scanning.</td>
</tr>
<tr>
<td>Network Content Inspection Pattern</td>
<td>The pattern used by the Network Content Inspection Engine to perform network scanning.</td>
</tr>
<tr>
<td>Network Content Correlation Pattern</td>
<td>The pattern used by the Network Content Correlation Engine that implements rules defined by Trend Micro.</td>
</tr>
<tr>
<td>Threat Correlation Pattern</td>
<td>The pattern used by Deep Discovery Inspector to perform threat correlation.</td>
</tr>
<tr>
<td>Threat Connect</td>
<td>Provides threat avoidance suggestions, details about individual threat types, and methods for removing threats from an infected system.</td>
</tr>
<tr>
<td>Widget Framework</td>
<td>Provides a template for Deep Discovery Inspector widgets.</td>
</tr>
<tr>
<td>Deep Discovery Inspector Firmware</td>
<td>The program file used by Deep Discovery Inspector.</td>
</tr>
</tbody>
</table>

**Tip:** Trend Micro recommends using the Firmware Update screen when updating the firmware.
Component Update Methods

Use one of these methods to update components:

**TABLE 5-3. Update methods**

<table>
<thead>
<tr>
<th>METHOD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
**Note:** Deep Discovery Inspector updates all components. You cannot update components individually.  
Select Administration > Global Settings > Update Components > Source on the web console to update the Deep Discovery Inspector firmware. For details, see Firmware Update on page 6-32. |
| Scheduled update | Select Administration > Global Settings > Update Components > Scheduled on the web console to configure an update schedule. Deep Discovery Inspector automatically checks the update source at the specified frequency. Scheduling updates allows you to "set it and forget it". See Scheduled Updates on page 5-15. |

Update Tasks

To update all components, review these procedures:

- Proxy Settings on page 5-8
- Update Source on page 5-15
- Manual Updates on page 5-14
- Scheduled Updates on page 5-15
- Firmware Update on page 6-32
Manual Updates

Deep Discovery Inspector allows on-demand component updates. Use this feature during outbreaks or when updates do not arrive according to a fixed schedule.

The following details appear in the Manual Download screen:

**TABLE 5-4. Details in the Manual Download screen**

<table>
<thead>
<tr>
<th>DETAILS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>The component name</td>
</tr>
<tr>
<td>Current Version</td>
<td>The version number of each component currently used by the product</td>
</tr>
<tr>
<td>Latest Version</td>
<td>The latest version available on the server</td>
</tr>
<tr>
<td>Last Updated</td>
<td>The date and time of the last update</td>
</tr>
</tbody>
</table>

**To perform manual updates:**

**PATH:** ADMINISTRATION > GLOBAL SETTINGS > UPDATE COMPONENTS > MANUAL

1. Deep Discovery Inspector automatically checks which components need updating. Any components that need updating appear in red.
2. Click the Update button.

Deep Discovery Inspector components update; when update is complete, an **All components are up-to-date** message appears.

**Note:** If the Network Content Inspection Engine and firmware were updated during a scheduled update, a notification email reminder to restart Deep Discovery Inspector is sent. Restart the product. When Deep Discovery Inspector starts, it checks the integrity of its configuration files. The product console password may reset if the configuration file containing password information is corrupted. If you are unable to log on to the console using your preferred password, log on using the default password **admin.**
Scheduled Updates

Configuring scheduled updates ensures that Deep Discovery Inspector components are the most current.

**Tip:** Schedule updates during off-peak hours.

### To configure scheduled updates:

**Path:** Administration > Global Settings > Update Components > Scheduled

1. Select **Enable Scheduled Updates**.
2. Select the update schedule based on **Minute, Hour, Day, or Week** and specify the time or day.

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

3. Click **Save**.

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

Update Source

Deep Discovery Inspector downloads components from the Trend Micro ActiveUpdate server, the default update source. Deep Discovery Inspector can be configured to download components from another update source specifically set up in your organization.
To configure the update source:

**PATH:** ADMINISTRATION > GLOBAL SETTINGS > UPDATE COMPONENTS > SOURCE

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

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

2. (Optional) Enable **Retry unsuccessful updates** and specify **Number of retry attempts** and **Retry interval**.

3. Click **Save**.
Configuring Product Settings

Configure these Deep Discovery Inspector settings as needed.

The topics discussed in this chapter are:

- Deep Discovery Inspector Notifications on page 6-2
- Network Configuration on page 6-8
- Detection Settings on page 6-13
- Integration with Trend Micro Products and Services on page 6-22
- Global Settings on page 6-25
Deep Discovery Inspector Notifications

Deep Discovery Inspector can be configured to send notifications for certain network events. These notifications are delivered to the intended recipients through email, in plain text format. To configure email settings, see Delivery Options on page 6-7.

Threshold-based Notifications

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

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Events Notification</td>
<td>Notification is sent when outbound or inbound traffic meets a set threshold for certain threat events. See Notification for Threat Events on page 6-3.</td>
</tr>
<tr>
<td>Detection of High Risk Hosts</td>
<td>Notification is sent when the number of detections per IP address exceeds the threshold. See Notification for Detection of High Risk Hosts on page 6-4.</td>
</tr>
<tr>
<td>Detection of Suspicious Hosts</td>
<td>Notification is sent when the number of suspicious hosts exceeds the threshold. See Notification for Detection of Suspicious Hosts on page 6-5.</td>
</tr>
<tr>
<td>High Network Traffic</td>
<td>Notification is sent when network traffic exceeds the normal traffic pattern. See Notification for High Network Traffic on page 6-6.</td>
</tr>
<tr>
<td>File Analysis Status</td>
<td>Notification is sent when the file analysis fails. See Notification for File Analysis Status on page 6-7.</td>
</tr>
</tbody>
</table>
Notification for Threat Events

When Deep Discovery Inspector detects that the threat events count of configured criteria (traffic direction, threat type, and time range) has reached a threshold, it sends email notification to alert users how many threat events of each configured threat type have been detected.

To configure notifications for threat events

PATH: ADMINISTRATION > NOTIFICATIONS > NOTIFICATION SETTINGS > THREAT EVENTS

1. At the Threat Events Notification settings screen, check **Notify Administrator**. Default notification settings are enabled.

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

2. To change the default settings, set the threshold for outbound and inbound traffic.
   - **Outbound traffic** means detections from monitored networks
   - **Inbound traffic** means detections from outside the network

3. Select which types of threat events to detect.

4. Click **Save**.

5. Verify that the email notification settings are correct. See *Delivery Options* on page 6-7.

To disable notifications:

PATH: ADMINISTRATION > NOTIFICATIONS > NOTIFICATION SETTINGS > THREAT EVENTS NOTIFICATION

1. Clear **Notify Administrator**.

2. Click **Save**.
Notification for Detection of High Risk Hosts

Deep Discovery Inspector can send an email when it detects high risk hosts. Use the Detection of High Risk Hosts notification screen to configure the notifications sent to the designated individuals. These notifications contain information that can help determine why a client is reporting a high number of detections and how to resolve this issue before it becomes the source of an outbreak.

To configure notifications for detection of high risk hosts:

**Path:** Administration > Notifications > Notification Settings

1. Select the Detection of High Risk Hosts option.
   Default notification settings are enabled.

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

2. At the High Risk Host Notification settings screen, check **Notify Administrator**.
3. Select a Sending Interval (1 minute to 30 days).
4. Verify that the email notification settings are correct. See *Delivery Options* on page 6-7.
5. Click **Save**.
   Notification settings are enabled.

To disable notifications:

**Path:** Administration > Notifications > Notification Settings > Detection of High Risk Hosts

1. Uncheck **Notify Administrator**.
2. Click **Save**.

**Notification Exclusion List**

To add known safe IP addresses to the High Risk Hosts Notification Exclusion List type either an IP address or address range in the corresponding fields, then click **Add**.

The IP address/address range appears in the Defined IP Addresses list.
Notification for Detection of Suspicious Hosts

Deep Discovery Inspector can send an email when it detects suspicious hosts. Deep Discovery Inspector classifies these clients as suspicious when they exceed the specified number of detections. Use the Detection of Suspicious Hosts notification screen to configure the notifications sent to the designated individuals. These notifications contain information that can help determine why a host is reporting a high number of detections and how to resolve this issue before it becomes the source of an outbreak.

To configure notifications for detection of suspicious hosts:

**PATH:** ADMINISTRATION > NOTIFICATIONS > NOTIFICATION SETTINGS

1. Select the Detection of Suspicious Hosts option.
2. At the Suspicious Host Notification settings screen, check **Notify Administrator.** Default notification settings are enabled.

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

3. To change the default settings, set the threshold for number of detections per IP address.
4. Verify that the email notification settings are correct. See *Delivery Options* on page 6-7.
5. Click **Save.**

To disable notifications:

**PATH:** ADMINISTRATION > NOTIFICATIONS > NOTIFICATION SETTINGS > DETECTION OF SUSPICIOUS HOSTS

2. Click **Save.**
Notification for High Network Traffic

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

To configure notifications for detection of high network traffic:

**PATH:** ADMINISTRATION > NOTIFICATIONS > NOTIFICATION SETTINGS

1. Select the High Network Traffic option.
2. At the High Traffic Usage Notification settings screen, check Notify Administrator.
   Default notification settings are enabled.

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

3. Click the Auto-Detect icon to allow Deep Discovery Inspector to define the normal traffic threshold or manually identify the traffic threshold at certain hours of the day.

   **Note:** The traffic threshold default unit is 1GB.

   **Note:** The amount of network traffic is rounded to the nearest whole number. For example, 1.2GB displays as 2GB and 2.6GB displays as 3GB.

4. Click Save. The Normal Traffic Pattern display is updated.
5. Verify that the email notification settings are correct. See Delivery Options on page 6-7.

To disable notifications:

**PATH:** ADMINISTRATION > NOTIFICATIONS > NOTIFICATION SETTINGS > HIGH NETWORK TRAFFIC

2. Click Save.
Notification for File Analysis Status

When file analysis fails, a notification is sent to a designated individual.

To configure notifications for file analysis failure:

**PATH:** ADMINISTRATION > NOTIFICATIONS > NOTIFICATION SETTINGS

1. Select the File Analysis Status option.
2. At the File Analysis Status Notification settings screen, select **Notify Administrator**.
   Default notification settings are enabled.

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

3. Change the sending interval, as needed, to a time period from 1 hour to 30 days.
4. Click **Save**.
5. Verify that the email notification settings are correct. See *Delivery Options* on page 6-7.

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.

Email Settings

**To configure the email settings:**

**PATH:** ADMINISTRATION > NOTIFICATIONS > DELIVERY OPTIONS > EMAIL SETTINGS

1. For **Notification recipient**, type the recipient's email address.

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

2. For **Sender's email address**, type the sender's email address.
3. Type the SMTP server name or IP address and port.
4. If the SMTP server requires authentication, specify the user name and password for the SMTP server.

Tip: Ensure that the Deep Discovery Inspector IP address is added to the SMTP relay list.

5. Specify the maximum number of notifications and the number of minutes to check the mail queue.

Tip: Trend Micro recommends using the default settings.

6. Click Save.

**Network Configuration**

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

See the following topics for details:
- *Monitored Networks* on page 6-9
- *Registered Domains* on page 6-10
- *Registered Services* on page 6-11

Network configuration settings can be replicated from one Deep Discovery Inspector device to another by exporting the settings to a file and then importing the settings file to other Deep Discovery Inspector devices. For details, see *Export/Import Configuration* on page 6-12.
Monitored Networks

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

**To add monitored networks:**

**PATH:** ADMINISTRATION > NETWORK CONFIGURATION > MONITORED NETWORK

1. Click **Add**.
   
The Add Monitored Network Group screen appears.

2. Specify a **Group name**.

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

3. Specify an **IP address range** in the text box (up to 1,000 IP address ranges).

   Deep Discovery Inspector comes with a monitored network called **Default**, which contains the following IP address blocks reserved by the Internet Assigned Numbers Authority (IANA) for private networks:
   
   - 10.0.0.0 - 10.255.255.255
   - 172.16.0.0 - 172.31.255.255
   - 192.168.0.0 - 192.168.255.255
   
   a. If you did not remove **Default**, you do not need to specify these IP address blocks when adding a new monitored network.
   b. Use a dash to specify an IP address range.
   c. Use a slash to specify the subnet mask for IP addresses.
      Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24.

4. Select the **Network zone** of network group.

   **Note:** Selecting **Trusted** means this is a secure network and selecting **Untrusted** means there is a degree of doubt about the security of the network.
5. Click Add.
6. Click Save.

To remove monitored networks:
PATH: ADMINISTRATION > NETWORK CONFIGURATION > MONITORED NETWORK
1. Select the Group name to be removed.
2. Click Delete.

Registered Domains

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

Add only trusted domains (up to 1,000 domains) to ensure the accuracy of your network profile.

Deep Discovery Inspector supports suffix-matching for registered domains (adding domain.com adds one.domain.com, two.domain.com, and so on).

To add registered domains:
PATH: ADMINISTRATION > NETWORK CONFIGURATION > REGISTERED DOMAINS
1. Specify a domain name to be registered.

Note: Registered domain names appear in the Defined Registered Domains section.

2. (Optional) Click Analyze to display a list of domains that can be added to the list.
3. Click Add.

To remove registered domains:
PATH: ADMINISTRATION > NETWORK CONFIGURATION > REGISTERED DOMAINS
1. In the Defined Registered Domains section select the domain(s) to be removed.
2. Click Delete.
Registered Services

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

Add only trusted services (up to 1,000 services) to ensure the accuracy of your network profile.

To add a registered service:

PATH: ADMINISTRATION > NETWORK CONFIGURATION > REGISTERED SERVICES

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

2. (Optional) Click Analyze to display a list of services that can be added to the list.

3. Specify a server name.

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

**Note:** Registered service names appear in the Defined Registered Services section.
4. Specify an IP address.

   **Note:** IP address ranges cannot be specified.

5. Click Add.

**To remove registered services:**

**PATH:** ADMINISTRATION > NETWORK CONFIGURATION > REGISTERED SERVICES

1. In the Defined Registered Services section select the service to be deleted.
2. Click Delete.

**Export/Import Configuration**

Network configuration settings include: monitored networks, registered domains, and registered services. To replicate these settings from one Deep Discovery Inspector device to another, export the settings to a file and then importing the file to other Deep Discovery Inspector appliances.

The default file name is cav.xml, which can be changed to a preferred file name.

   **Note:** To replicate Deep Discovery Inspector settings, in addition to network configuration settings, see Backup/Restore Appliance Configuration on page 6-26.

**To replicate and export network configuration settings (Device 1):**

**PATH:** ADMINISTRATION > NETWORK CONFIGURATION > EXPORT/IMPORT CONFIGURATION

1. Under Export Configuration, click Export.

   A message prompts you to open or save the cav.xml file.
2. Click Save, browse to the target location of the file, and click Save.

**To replicate and import network configuration settings (Device 2):**

**PATH:** ADMINISTRATION > NETWORK CONFIGURATION > EXPORT/IMPORT CONFIGURATION

1. Under Export Configuration, click Export.

   A message prompts you to open or save the cav.xml file.
2. Click Save, browse to the target location of the file, and click Save.
This backs up the current network configuration settings.

3. Under **Import Configuration**, click **Browse**.
4. Locate the cav.xml file and click **Open**.
5. Click **Import**.

**Detection Settings**

Detections establish filters and exclusions for the Deep Discovery Inspector network detection features.

**Threat Detections**

Enable or disable the following features.

**Table 6-3. Threat detection features**

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Detections</td>
<td>Detects both known and potential threats. Trend Micro enables this feature by default.</td>
</tr>
<tr>
<td>Outbreak Containment Services</td>
<td>Enables Deep Discovery Inspector to record detection information in the logs and block network traffic. Trend Micro enables this feature by default.</td>
</tr>
<tr>
<td>Block Traffic</td>
<td>Resets network connections of unknown malware when detected. Trend Micro disables this feature by default.</td>
</tr>
</tbody>
</table>

**To configure threat detection:**

**PATH:** **Administration > Detection Settings > Threat Detections**

1. Enable the **Enable All Threat Detections** option.
2. Under **Threat Detections**, enable **Enable threat detections** option.
   - Default settings are enabled.
3. Under Outbreak Containment Services, select:
Enable outbreak detection (does not block traffic) or
Enable outbreak detection and block traffic (blocks traffic)

4. Click Save.

To disable detections:
PATH: ADMINISTRATION > DETECTION SETTINGS > THREAT DETECTIONS

1. Clear Enable All Threat Detections.
2. Click Save.

Application Filters

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

Enable detection for the following applications:

<table>
<thead>
<tr>
<th>APPLICATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant Messaging</td>
<td>A popular means of communicating and sharing information and files with contacts</td>
</tr>
<tr>
<td>P2P Traffic</td>
<td>Using peer-to-peer protocol to share files from one computer to another</td>
</tr>
<tr>
<td>Streaming Media</td>
<td>Audio-visual content that plays while downloading</td>
</tr>
</tbody>
</table>

To configure Application Filters settings:
PATH: ADMINISTRATION > DETECTION SETTINGS > APPLICATION FILTERS

1. Enable detection for Instant Messaging.
   a. Select the Instant Messaging check box.
   b. Select the specific instant message applications for detection.
Tip: Use the CTRL key to select one or multiple protocol types.

c. Click the double arrow to move the selected instant message applications under Selected Instant Messaging applications.

2. Enable detection for P2P Traffic.
   a. Select the P2P Traffic check box.
   b. Select the specific peer-to-peer applications for detection.

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

c. Click the double arrow to move the selected peer-to-peer applications under Selected Peer-to-Peer applications.

3. Enable detection for Streaming Media.
   a. Select the Streaming Media check box.
   b. Select the specific streaming media applications for detection.

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

c. Click the double arrow to move the selected streaming media applications under Selected streaming media applications.

4. Click Save.

Smart Protection Technology

Trend Micro smart protection technology is a next-generation, in-the-cloud protection solution providing File and Web Reputation Services. By leveraging the Web Reputation Service, Deep Discovery Inspector can obtain reputation data for websites that users are attempting to access. Deep Discovery Inspector logs URLs that smart protection technology verifies to be fraudulent or known sources of threats and then uploads the logs for report generation.
Note: Deep Discovery Inspector does not use the File Reputation Service that is part of smart protection technology.

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

**TABLE 6-5. Smart protection sources**

<table>
<thead>
<tr>
<th>BASIS OF COMPARISON</th>
<th>TREND MICRO SMART PROTECTION NETWORK</th>
<th>SMART PROTECTION SERVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>A globally scaled, Internet-based infrastructure that provides File and Web Reputation Services to Trend Micro products that leverage smart protection technology</td>
<td>Provides the same File and Web Reputation Services offered by Smart Protection Network but is intended to localize these services to the corporate network to optimize efficiency</td>
</tr>
<tr>
<td>Administration</td>
<td>Trend Micro hosts and maintains this service.</td>
<td>Trend Micro product administrators install and manage this server.</td>
</tr>
<tr>
<td>Connection protocol</td>
<td>HTTPS</td>
<td>HTTP</td>
</tr>
<tr>
<td>Usage</td>
<td>Use if you do not plan to install Smart Protection Server. To configure Smart Protection Network as source, see Web Reputation on page 6-17.</td>
<td>Use as primary source and the Smart Protection Network as an alternative source. For guidelines in setting up Smart Protection Server and configuring it as source, see Setting Up Smart Protection Server on page 6-17.</td>
</tr>
</tbody>
</table>
Setting Up Smart Protection Server

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

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

Installation reminders and recommendations:

- For information on the Smart Protection Server versions compatible with Deep Discovery Inspector, see Integration with Trend Micro Products and Services on page 6-22.
- For installation instructions and requirements, refer to the Installation and Upgrade Guide for Trend Micro Smart Protection Server.
- Smart Protection Server and the VMware ESX/ESXi server (which hosts the Smart Protection Server) require unique IP addresses. Check the IP addresses of the VMware ESX/ESXi server and Deep Discovery Inspector to ensure that none of these IP addresses is assigned to the Smart Protection Server.
- If you have previously installed a Smart Protection Server for use with another Trend Micro product, you can use the same server for Deep Discovery Inspector. While several Trend Micro products can send queries simultaneously, the Smart Protection Server may become overloaded as the volume of queries increases. Ensure that the Smart Protection Server can handle queries coming from different products. Contact your support provider for sizing guidelines and recommendations.
- Trend Micro recommends installing multiple Smart Protection Servers for failover purposes. Deep Discovery Inspector checks the Smart Protection Server list configured in the web console to determine which server to connect to first, and the alternative servers if the first server is unavailable.

Configure Smart Protection Server settings from the Deep Discovery Inspector console. For details, see Web Reputation on page 6-17, from step 3.

Web Reputation

Deep Discovery Inspector leverages Trend Micro smart protection technology, a cloud-based infrastructure that determines the reputation of websites users are attempting to access. Web reputation requires smart protection technology, see Setting Up Smart Protection Server on page 6-17 for setup instructions. Deep Discovery Inspector logs URLs that smart protection technology verifies to be fraudulent or known sources of threats. The product then uploads the logs for report generation.
To configure web reputation settings:

**PATH:** ADMINISTRATION > DETECTION SETTINGS > WEB REPUTATION

1. Check **Enable Web Reputation**.
2. Select the Smart Protection Source.

   Deep Discovery Inspector connects to a smart protection source to obtain web reputation data.

   **Trend Micro Smart Protection Network** is a globally-scaled Internet-based infrastructure that provides reputation services to Trend Micro products that leverage smart protection technology. Deep Discovery Inspector securely connects to the Smart Protection Network using HTTPS. Select this option if you do not plan to set up a Smart Protection Server.

   **Smart Protection Server** provides the same file and web reputation services offered by the Smart Protection Network. Smart Protection Server is intended to optimize efficiency by localizing these services to the corporate network. As a Trend Micro product administrator, you need to set up and maintain this server. Select this option if you have already done so.

3. To select **Smart Protection Server**:
   a. Type the Smart Protection Server’s IP address.
      i. Obtain the IP address by navigating to **Smart Protection > Reputation Services > Web Reputation** tab on the Smart Protection Server console. The IP address forms part of the URL listed in the screen.
   b. Click **Test Connection** to check if connection to the server can be established.
   c. Type a description for the server.
   d. Select whether to query the Smart Protection Network if the Smart Protection Server cannot determine a URL’s reputation.
Note: The Smart Protection Server may not have reputation data for all URLs because it cannot replicate the entire Smart Protection Network data. When updated infrequently, the Smart Protection Server may also return outdated reputation data.

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

e. If you enable this option, do the following to optimize web reputation queries:
   i. On the Smart Protection server console, navigate to Smart Protection > Reputation Services > Web Reputation tab > Advanced Settings section. Disable *Use only local resources, do not send queries to Smart Protection Network.*

Note: This option prevents the Smart Protection Server from obtaining data from Smart Protection Network.

ii. Update the Smart Protection Server regularly.

Note: Disable this option if you do not want your organization's data to be transmitted externally.

f. Select *Connect through a proxy server* if Proxy Settings for Deep Discovery Inspector have been configured for use with Smart Protection Server connections.

Note: If proxy settings are disabled, Smart Protection Servers that connect through the proxy server will connect to Deep Discovery Inspector directly. Under the *Proxy Connection* column, the status is *Proxy Unavailable.*

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

**h. Add more servers.**

**Note:** Up to 10 servers can be added. If additional servers are added, Deep Discovery Inspector connects to these servers in the order in which they appear in the list.

**Tip:** Trend Micro recommends adding multiple Smart Protection Servers for failover purposes. If Deep Discovery Inspector is unable to connect to a server, it attempts to connect to the other servers on the Smart Protection Server List.

i. Use the arrows under the Order column to move servers up and down the list.

4. Click **Enable Smart Feedback (recommended)** to send threat information to the Trend Micro Smart Protection Network. This allows Trend Micro to identify and address new threats. Participation in Smart Feedback authorizes Trend Micro to collect certain information from your network, which is kept in strict confidence. Information includes:
   - This product's name and version
   - URLs suspected to be fraudulent or possible sources of threats
   - URLs associated with spam or possibly compromised
   - Malware name for URLs that harbor malware.

5. Click **Save**.

**To manage the Smart Protection Server list:**

**Path:** Administration > Detection Settings > Web Reputation

1. To verify the connection status with a Smart Protection Server, click **Test Connection**.

2. To modify server settings:
   a. Click the server address.
b. In the window that appears, modify the server's IP address, description, and settings.

c. After specifying a new IP address, click Test Connection to confirm the connection.

d. Click OK.

3. To remove a server from the list, click Delete.

4. Click Save.

Detection Exclusion List

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

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

To configure the detection exclusion list for threats:

PATH: ADMINISTRATION > DETECTION SETTINGS > DETECTION EXCLUSION LIST

1. Select the Threat Detections tab.

2. Specify a unique name for easy identification.

3. Specify an IP address or IP address range in the text field.

   a. Use a dash to specify an IP address range

   b. Use a slash to specify the subnet mask for IP addresses
      Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24.

4. Click Add.

5. To remove an item from the Exclusion List, select the item and click Delete.

To configure the exclusion list for Outbreak Containment Services:

PATH: ADMINISTRATION > DETECTION SETTINGS > DETECTION EXCLUSION LIST

1. Select the Outbreak Containment Services tab.

2. Specify a unique name for easy identification.
3. Specify an IP address or IP address range in the text field.
   a. Use a dash to specify an IP address range.
   b. Use a slash to specify the subnet mask for IP addresses.
      Example: 192.168.1.0/255.255.255.0 or 192.168.1.0/24.
4. Click Add.
5. To remove an item from the Exclusion List, select the item and click Delete.

Integration with Trend Micro Products and Services

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

<table>
<thead>
<tr>
<th>PRODUCT / SERVICE</th>
<th>DESCRIPTION</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network VirusWall Enforcer</td>
<td>Regulates network access based on the security posture of endpoints. For details, see Mitigation Device Settings on page 6-36.</td>
<td>3.0 with Patch 1 and newer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.0 Service Pack 1 with Patch 1</td>
</tr>
<tr>
<td>Smart Protection Network</td>
<td>Provides the Web Reputation Service, which determines the reputation of websites that users are attempting to access. Smart Protection Network is hosted by Trend Micro. For details, see Smart Protection Technology on page 6-15.</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>
### TABLE 6-6.  Trend Micro products and services that integrate with Deep Discovery Inspector (Continued)

<table>
<thead>
<tr>
<th>PRODUCT/SERVICE</th>
<th>DESCRIPTION</th>
<th>VERSION</th>
</tr>
</thead>
</table>
| Smart Protection Server | Provides the same Web Reputation Service offered by Smart Protection Network.  
Smart Protection Server is intended to localize the service to the corporate network to optimize efficiency.  
For details, see Smart Protection Technology on page 6-15. | 2.0                      |
| Threat Connect  | Provides details about detected threat behavior.                            | Not applicable           |
| Threat Management Services Portal (TMSP) | Receives logs and data from Deep Discovery Inspector, and then uses them to generate reports containing security threats and suspicious network activities, and Trend Micro recommended actions to prevent or address them.  
For details, see Threat Management Services Portal on page 6-39. | 2.6 (for the on-premise edition of TMSP)  
Not applicable for the Trend Micro hosted service |
| Threat Mitigation | Receives mitigation requests from Deep Discovery Inspector after a threat is detected.  
Threat Mitigator then notifies the Threat Management Agent installed on a host to run a mitigation task.  
For details, see Mitigation Device Settings on page 6-36. | 2.6 (recommended)        |
### TABLE 6-6. Trend Micro products and services that integrate with Deep Discovery Inspector (Continued)

<table>
<thead>
<tr>
<th>Product/Service</th>
<th>Description</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trend Micro Control Manager</td>
<td>A software management solution that gives you the ability to control antivirus and content security programs from a central location—regardless of the platform or the physical location of the program. For details, see Control Manager Settings on page 6-43.</td>
<td>5.5</td>
</tr>
<tr>
<td>Trend Micro Deep Discovery Advisor</td>
<td>Deep Discovery Advisor is designed to: • Collect, aggregate, manage, and analyze logs into a centralized storage space • Provide advanced visualization and investigation tools that monitor, explore, and diagnose security events within the corporate network Deep Discovery Advisor provides unique security visibility based on Trend Micro’s proprietary threat analysis and recommendation engines. For details, see the Deep Discovery Advisor Administrator’s Guide.</td>
<td>2.92</td>
</tr>
</tbody>
</table>
Global Settings

System Settings

The System Settings window allows the basic settings of Deep Discovery Inspector to be configured.

Basic settings include:
• Date, Time, and Language Settings
• Web Console Timeout
• Proxy Settings
• Backup/Restore Appliance Configurations
• Import Custom Virtual Analyzer
• System Maintenance
• HTTPS Certificate
• Firmware Update
• System Update.

System Time

See Date, Time, and Language Settings on page 5-8.

Web Console Timeout

Configure how long Deep Discovery Inspector waits before logging out an inactive web console user session.

To configure web console timeout settings:

Path: Administration > Global Settings > System Settings > Web Console Timeout

1. At Timeout Settings, type the number of minutes (1-30) prior to inactivity logoff.
2. Click Save.
Note: The default web console timeout is 30 minutes.

Proxy Settings

See Proxy Settings on page 5-8.

Backup/Restore Appliance Configuration

Configuration settings include both Deep Discovery Inspector and network configuration settings. Back up configuration settings by exporting them to an encrypted file; this file can be imported to restore settings if needed.

Deep Discovery Inspector can be reset by restoring the default settings that shipped with the product.

Most or all settings of the following screens cannot be backed up:

- Virtual Analyzer Settings
- Threat Management Services Portal
- Mitigation Device Settings
- Control Manager Settings
- Appliance IP Settings
- Licenses and Activation Codes
- Smart Protection Settings in the Web Reputation screen

The encrypted file cannot be modified.

Importing an encrypted file overwrites all the current settings on Deep Discovery Inspector.

An encrypted file can also be used to replicate settings on another Deep Discovery Inspector.
To back up settings to an encrypted file:

**PATH: Administration > Global Settings > System Settings > Backup/Restore Appliance Configurations**

1. At Backup Configuration click Backup.
   A file download screen opens.
2. Click Save, browse to the target location of the file, and click Save.
3. Click Find to find a program to open the file.

To import an encrypted file:

**PATH: Administration > Global Settings > System Settings > Backup/Restore Appliance Configurations**

1. Before importing a file, back up the current configurations by performing the steps under To back up settings to an encrypted file: on page 6-27.
2. At Restore Configuration click Browse.
   The Choose File to Upload screen appears.
3. Select the encrypted file to import and click Restore Configuration.
   A confirmation message appears.
4. Click OK. Deep Discovery Inspector restarts after importing the configuration file.

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

To restore the default settings that shipped with the product:

**PATH: Administration > Global Settings > System Settings > Backup/Restore Appliance Configurations**

1. Before restoring settings, back up the current configurations by performing the steps under To back up settings to an encrypted file: on page 6-27.
2. Click Reset to Default Settings.
   A confirmation message appears.
3. Click OK.
Deep Discovery Inspector restarts after restoring the default configuration settings.

4. Wait one minute after re-start to log onto the web console.

---

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

---

**Import Custom Virtual Analyzer**

The custom Virtual Analyzer is a virtualized environment designed to allow simulation of malware behavior and inspection of untrusted programs. For details on creating a custom Virtual Analyzer, see *Converting a VMware Image* on page A-2 or *Using VirtualBox to Export an OVA Image* on page A-33. Virtual Analyzer information and status are displayed on this screen.

**To import a custom Virtual Analyzer using the manual submission tool:**

**Path:** Administration > Global Settings > System Settings > Import Custom Virtual Analyzer

1. To establish a connection to Deep Discovery Inspector, select **Click Here** on Step 1.

2. To install the Virtual Analyzer Image Upload Tool, select **Click Here** on Step 2.
   A message regarding ImageUpload.exe appears.

3. Select Run or Save.
   a. **Run:**
      i. At the Deep Discovery Inspector Virtual Analyzer Image Upload Tool screen, type the IP address of server used to access Deep Discovery Inspector.
      ii. Browse to the custom Virtual Analyzer image file.
      iii. Click **Upload**.
      The custom Virtual Analyzer image is uploaded.

   b. **Save:**
i. Click the dropdown menu and select either **Save As** or **Save and run**.

**Note:** Clicking the **Save** button without using the dropdown menu is the same as selecting **Run**. See **Run** on page 6-28.

**Note:** Click **View downloads** to review/select previously downloaded images.

ii. **Save As**: Change the name of the Upload Tool and click **Save**.

iii. **Save and run** is the same as selecting **Run**. See **Run** on page 6-28.

**Note:** If the upload times out or encounters an error, click **Reset** and restart image upload. Repeats steps 1 and 2.

**To import a custom Virtual Analyzer from an FTP/HTTP server:**

**PATH:** ADMINISTRATION > GLOBAL SETTINGS > SYSTEM SETTINGS > IMPORT CUSTOM VIRTUAL ANALYZER

1. On the Import Custom Virtual Analyzer screen, click the **Import from FTP/HTTP** tab.

2. Type the URL for the image location.
   
   **Example:**
   
   ftp://***/**OVA or http://**/**OVA

3. Select either a Username/Password combination or check Anonymous Login.
   
   **Note:** Use Anonymous Login only if the ftp or http site supports this function.

4. Click **Import**.
   
   The image is imported.
   
   An **Import Done** message appears.

   **Note:** This may take up to 10 minutes to complete.
System Maintenance

Enable or disable a SSH connection, shut down or restart Deep Discovery Inspector or its associated services from the screen on the product console.

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

To enable/disable an SSH connection:

Path: Administration > Global Settings > System Settings > System Maintenance

1. Select Enable/Disable under SSH Connection.

   An SSH connection is enabled or disabled.

   Note: For added security, this option is not enabled by default; it must be manually enabled.

To shut down Deep Discovery Inspector:

Path: Administration > Global Settings > System Settings > System Maintenance

1. Click Shut down.

2. (Optional) Specify a reason for the shut down, in the comment field.

3. Click OK.

To restart Deep Discovery Inspector or its services:

Path: Administration > Global Settings > System Settings > System Maintenance

1. Click Restart.
   a. To restart services, click Service.
   b. To restart Deep Discovery Inspector, click System.

2. (Optional) Specify a reason for restarting the services, in the Comment field.

3. Click OK.
HTTPS Certificate

Verify that the HTTPS certificate details are accurate. Replace as needed.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Certificate version number</td>
</tr>
<tr>
<td>Serial number</td>
<td>Used to uniquely identify the certificate</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>The algorithm used to create the signature</td>
</tr>
<tr>
<td>Issuer</td>
<td>The entity that verified the information and issued the certificate</td>
</tr>
<tr>
<td>Valid from</td>
<td>The date the certificate is first valid</td>
</tr>
<tr>
<td>Valid to</td>
<td>The certificate expiration date</td>
</tr>
<tr>
<td>Subject</td>
<td>The person or entity identified</td>
</tr>
<tr>
<td>Public Key</td>
<td>The 82-bit public key, used for encryption</td>
</tr>
</tbody>
</table>

To replace the certificate:

**PATH: ADMINISTRATION > GLOBAL SETTINGS > SYSTEM SETTINGS > HTTPS CERTIFICATE**

1. At the HTTPS Certificate screen, click Replace Certificate.
   The Import Certificate screen appears.
2. At the Import Certificate screen, click Browse to navigate to, and select, a new certificate; click Import.
   A new certificate is imported.
3. Log on to Deep Discovery Inspector from another browser to verify new certificate.

**Note:** Deep Discovery Inspector does not need to be restarted.
Firmware Update

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

**Before updating the firmware:**

2. If you have registered Deep Discovery Inspector to Control Manager, record the Control Manager registration details.

   **Note:** You need to re-register to Control Manager after the firmware update is complete.

3. Download the Deep Discovery Inspector firmware image from the Trend Micro website or obtain the image from your Trend Micro reseller or support provider.
4. Save the image to any folder on a computer.

**To update the firmware:**

**Path:** Administration > Global Settings > System Settings > Firmware Update

1. Click **Browse** and locate the folder to which you saved the firmware image (the image file has an .R extension).
2. Click **Upload Firmware**.

   The Migration configuration option appears.
3. Enable this option to retain the current product settings after the update, or disable it to revert to the product’s default settings after the update.

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

4. Click **Continue**.

   Deep Discovery Inspector restarts after the update.

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

**After updating the firmware:**

If Deep Discovery Inspector is registered to Control Manager, register the product again. For details, see *Control Manager Settings* on page 6-43.

**System Update**

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

**System Update Types**

Trend Micro may release the following types of system updates:

<table>
<thead>
<tr>
<th>TABLE 6-8. System updates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYSTEM UPDATE</strong></td>
</tr>
<tr>
<td>Hot fix</td>
</tr>
<tr>
<td>Security patch</td>
</tr>
<tr>
<td>Patch</td>
</tr>
</tbody>
</table>
Your vendor or support provider may contact you when these items become available. Check the Trend Micro website for information on new hot fix, patch, and service pack releases:

http://www.trendmicro.com/download

System Update Rollback

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

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

Before performing a system update:

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

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

2. Read the readme file carefully before applying the system update.

   **Note:** All releases include a readme file that contains installation, deployment, and configuration information.
Tip: The readme file should indicate if a system update requires Deep Discovery Inspector to restart. If a restart is required, ensure that all tasks on the console have been completed before applying the update.

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

To apply system updates:

Path: Administration > Global Settings > System Settings > System Update

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

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

3. If the upload was successful, check the Uploaded System Update Details section. This section indicates the build number for the system update that you just uploaded and if a restart is required.

Note: You will be redirected to the web console's logon screen after the update is applied.

4. If a restart is required, finish all tasks on the web console before proceeding.
5. Click Continue to apply the system update.

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

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

6. Skip this step if a restart is not required.
If a restart is required:

a. Log on to the web console.

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

c. Navigate back to the System Update screen.

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

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

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

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

b. Click **Roll Back**.

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

### Component Updates

See **Component Updates** on page 5-11.

### Mitigation Device Settings

Mitigation devices receive threat information gathered by Deep Discovery Inspector. These devices work with an Agent program installed on an endpoint to resolve threats. Mitigation devices with network access control function may prevent the endpoint from accessing the network until the endpoint is free of threats.
Mitigation Settings

Register Deep Discovery Inspector with up to 200 mitigation devices. For information on the device versions compatible with Deep Discovery Inspector, see Integration with Trend Micro Products and Services on page 6-22.

To enable/disable mitigation device enforcement:
PATH: ADMINISTRATION > GLOBAL SETTINGS > MITIGATION DEVICE SETTINGS > MITIGATION SETTINGS

Select Enable/Disable, at Mitigation Device Enforcement, to enable or disable the sending of mitigation requests.
Mitigation device enforcement is enabled/disabled.

Note: Select this option after registering Deep Discovery Inspector to at least one mitigation device.

To register Deep Discovery Inspector to mitigation devices:
PATH: ADMINISTRATION > GLOBAL SETTINGS > MITIGATION DEVICE SETTINGS > MITIGATION SETTINGS

1. Under Mitigation Device Registration, type the mitigation device Server name or IP address.
2. Type a Description for the device.
3. Specify IP address range.

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

4. Click Register.
The Cleanup Settings screen appears.
5. Select the types of security risks/threats to send to the mitigation device.
6. Click Apply.
To unregister Deep Discovery Inspector from mitigation devices:

**PATH:** ADMINISTRATION > GLOBAL SETTINGS > MITIGATION DEVICE SETTINGS > MITIGATION SETTINGS

1. Select the mitigation devices to unregister from.
2. Click **Delete**.

   The device is removed from the list.

---

**Note:** This task also triggers the mitigation device to remove Deep Discovery Inspector from its list of data sources.

---

**Mitigation Exclusion List**

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

Before configuring the mitigation exclusion list, ensure that Deep Discovery Inspector is registered to at least one mitigation device. For details, see *Mitigation Device Settings* on page 6-36.

A maximum of 100 entries can be added to the list.

**To configure the mitigation exclusion list:**

**PATH:** ADMINISTRATION > GLOBAL SETTINGS > MITIGATION DEVICE SETTINGS > MITIGATION EXCLUSION LIST

1. Type a name for the exclusion. Specify a meaningful name for easy identification. Example: "Lab Computers".
3. Click **Add**.
4. To remove an entry from the list, select the entry and click **Delete**.
Network Interface Settings

Network Interface Settings screen allows you to manage the product’s IP address and network interface ports. Deep Discovery Inspector requires its own IP address to ensure that the management port can access the product console. See Network Interface Settings on page 5-6.

Threat Management Services Portal

Threat Management Services Portal (TMSP) receives logs and data from registered products and creates reports to enable product users to respond to threats in a timely manner and receive up-to-date information about the latest and emerging threats.

Register Deep Discovery Inspector to TMSP to be able to

- Analyze Deep Discovery Inspector logs and data, including:
  - Detection
  - Application filter
  - URL filtering
  - Network configuration data, including monitored networks, registered domains, and registered services.

  **Note:** URL Filtering logs are not available on the Deep Discovery Inspector web console.

- Generate threat reports

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

Deep Discovery Inspector sends heartbeat messages to TMSP periodically. A heartbeat message informs TMSP that Deep Discovery Inspector is online.

Deep Discovery Inspector can use proxy server settings configured on the Proxy Settings screen to connect to TMSP.
Form Factor

Use TMSP as a Trend Micro hosted service and on-premise application installed on a bare metal server.

To install the on-premise edition of TMSP:

1. Refer to the TMSP Administrator’s Guide for installation and configuration instructions.
2. For information on the TMSP versions compatible with Deep Discovery Inspector, see Integration with Trend Micro Products and Services on page 6-22.
3. To use TMSP as a hosted service, ask your Trend Micro representative or support provider for the following information required to register Deep Discovery Inspector to TMSP:
   - IP addresses of TMSP log server and status server
   - Server authentication credentials

To configure TMSP settings:

PATH: ADMINISTRATION > GLOBAL SETTINGS > NETWORK INTERFACE SETTINGS > THREAT MANAGEMENT SERVICES PORTAL

1. Select Send logs and data to Threat Management Services Portal to register Deep Discovery Inspector to TMSP.

   Note: Disabling this option unregisters Deep Discovery Inspector from TMSP. Disable this option if you have TMSP:
   - as an on-premise application, manually remove Deep Discovery Inspector from the TMSP Registered Products screen.
   - as a hosted service, inform your Trend Micro representative about the unregistration.

2. Specify the log server for TMSP.
   a. To use TMSP as a hosted service, type the IP address or host name.
   b. To use TMSP as an on-premise application, type the IP address.
3. Select the protocol (SSH or SSL).
Configuring Product Settings

a. If a firewall has been set up, configure the firewall to allow traffic from Deep Discovery Inspector to TMSP through port 443 (for SSL) or port 22 (for SSH).

b. To use SSH and a Microsoft ISA Server, configure the tunnel port ranges on the ISA server to allow traffic from Deep Discovery Inspector to TMSP through port 22.

4. Specify how often to send logs to TMSP.

5. Specify the status server for TMSP.
   a. To use TMSP as a hosted service, type the IP address or host name.
   b. To use TMSP as an on-premise application, type the IP address.

**Note:** The status server receives the following information from Deep Discovery Inspector:

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

- Outbreak Containment Services

6. Type the server authentication credentials (user name and password). TMSP authenticates Deep Discovery Inspector using these credentials and then proceeds to accept logs and data.

7. Type the registration email address.

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

8. If you have configured Proxy Settings for Deep Discovery Inspector and want to use these settings for TMSP connections, select Connect through a proxy server.

9. To check whether Deep Discovery Inspector can connect to TMSP based on the settings you configured, click Test Connection.

10. Click Save if the test connection is successful.
SNMP Settings

Simple Network Management Protocol (SNMP) is used to manage distribution networks. Registering the SNMP server to check system status (system shutdown or start status), network card link up or link down, and component update status. The SNMP server has two modes: SNMP Trap and SNMP Agent. SNMP Trap allows a registered device to report its status to the SNMP Server. The SNMP Agent is an SNMP server registered to the device. Use SNMP Agent to obtain Deep Discovery Inspector system information (product version, CPU/Memory/Disk related info, Network Interface throughput).

**To configure SNMP Trap settings:**

**Path:** Administration > Global Settings > Network Interface Settings > SNMP Settings

1. At the SNMP Settings window, check **Enable SNMP trap**.
2. Type Community name and Server IP address.
3. Click **Save**.

**To configure SNMP Agent settings:**

**Path:** Administration > Global Settings > Network Interface Settings > SNMP Settings

1. At the SNMP Settings window, check **Enable SNMP agent**.
2. Type System location and System contact.
3. At Accepted Community Name(s), type Community name and click **Add to >**. Community Name is added to Community Name list.
4. At Trusted Network Management IP Address(es), type IP address and click **Add to >**.
5. Click **Save**. The IP address is added to the IP address list.
6. If needed, click **Export to MIB**, to save these settings for later use.
   a. Import the MIB settings file to the SNMP server.

Deep Discovery Inspector can be monitored from the SNMP server.
Control Manager Settings

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

For information on the Control Manager versions compatible with Deep Discovery Inspector, see Integration with Trend Micro Products and Services on page 6-22.

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

Control Manager Components

Table 6-9 lists the components that make up Control Manager.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Manager server</td>
<td>The computer upon which the Control Manager application is installed. This server hosts the web-based Control Manager product console</td>
</tr>
<tr>
<td>Management Communication Protocol (MCP) Agent</td>
<td>An application installed along with Deep Discovery Inspector that allows Control Manager to manage the product. The agent receives commands from the Control Manager server, and then applies them to Deep Discovery Inspector. It also collects logs from the product, and sends them to Control Manager. The Control Manager agent does not communicate with the Control Manager server directly. Instead, it interfaces with a component called the Communicator.</td>
</tr>
<tr>
<td>Communicator</td>
<td>The communications backbone of the Control Manager system; it is part of the Trend Micro Management Infrastructure. Commands from the Control Manager server to Deep Discovery Inspector, and status reports from Deep Discovery Inspector to the Control Manager server all pass through this component.</td>
</tr>
</tbody>
</table>
Use the Control Manager Settings screen on the Deep Discovery Inspector console to perform the following:

- Register to a Control Manager server.
- Verify that Deep Discovery Inspector can register to a Control Manager server.
- Check the connection status between Deep Discovery Inspector and Control Manager.
- Check the latest MCP heartbeat with Control Manager.
- Unregister from a Control Manager server.

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

### To register Deep Discovery Inspector to Control Manager:

**Path:** Administration > Global Settings > Network Interface Settings > Control Manager Settings

1. **Under Connection Settings** type the name that identifies Deep Discovery Inspector in the Control Manager Product Directory.

   **Note:** Specify a unique and meaningful name to help you quickly identify Deep Discovery Inspector.

2. **Under Control Manager Server Settings:**
   a. Type the Control Manager server IP address or host name.
b. Type the port number that the MCP agent uses to communicate with Control Manager.

c. Select **Connect using HTTPS** if the Control Manager security is set to medium (Trend Micro allows HTTPS and HTTP communication between Control Manager and the MCP agent of managed products) or high (Trend Micro only allows HTTPS communication between Control Manager and the MCP agent of managed products).

d. Type the user name and password for your IIS server in the **User name** and **Password** fields if your network requires authentication.

3. Select **Enable two-way communication port forwarding** if you use a NAT device, and type the NAT device’s IP address and port number in **Port forwarding IP address** and **Port forwarding port number**.

   **Note:** Deep Discovery Inspector uses the **Port forwarding IP address** and **Port forwarding port number** for two-way communication with Control Manager.

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

4. Select **Connect through a proxy server** if you have configured **Proxy Settings** for Deep Discovery Inspector and want to use these settings for Control Manager connections.

5. Click **Test Connection** to check whether Deep Discovery Inspector can connect to the Control Manager server based on the settings you specified.

6. Click **Register** if connection was successfully established.
To unregister Deep Discovery Inspector from Control Manager:

**PATH:** ADMINISTRATION > GLOBAL SETTINGS > NETWORK INTERFACE SETTINGS > CONTROL MANAGER SETTINGS

1. Under Connection Status, click the Unregister button.

**Note:** Use this option to unregister Deep Discovery Inspector to Control Manager or to register to another Control Manager.

To view the Deep Discovery Inspector status on the Control Manager console:

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

   https://<Control Manager server name>/WebApp/login.aspx

   Where <Control Manager server name> is the IP address or host name of the Control Manager server.

2. On Main Menu, click Products.
3. Select Managed Products from the list.
4. Verify that the Deep Discovery Inspector icon is displayed.

To manage the connection with Control Manager after registration:

**PATH:** ADMINISTRATION > GLOBAL SETTINGS > NETWORK INTERFACE SETTINGS > CONTROL MANAGER SETTINGS

1. Under Connection Status:
   
a. Verify that the product can connect to Control Manager.

b. If the product is not connected, restore the connection immediately.

c. Verify that the last heartbeat was received, which indicates the last communication between the MCP agent, Deep Discovery Inspector, and the Control Manager server.

2. To change settings after registration, click Update Settings to notify the Control Manager server of the changes.
3. To transfer control of Deep Discovery Inspector management to another Control Manager server, click **Unregister** and register Deep Discovery Inspector to the other server.

### Virtual Analyzer Settings

Use this option to enable or disable analysis of threat files.

**To submit files to the Virtual Analyzer:**

**Path:** Administration > Global Settings > Network Interface Settings > Virtual Analyzer Settings

1. Ensure that the management port can access the Internet; the virtual analyzer may need to query data through this port.

2. At the Virtual Analyzer Configuration window, check **Submit files to Virtual Analyzer**.

![Virtual Analyzer Configuration Window](image)

**FIGURE 6-1. Virtual Analyzer Configuration Window**

3. Select an analysis module.
   
   a. For Internal Analyzer: 
i. Select a Network Type. See Analyzer Network Types on page 6-48.

**TABLE 6-10. Analyzer Network Types**

<table>
<thead>
<tr>
<th>MODULE OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Network</td>
<td>Select this network type to direct virtual analyzer traffic through a management port.</td>
</tr>
<tr>
<td>Specified Network</td>
<td>Select this network type to configure a specific port for virtual analyzer traffic. Ensure that the port is able to connect to an outside network directly.</td>
</tr>
<tr>
<td>Isolated Network</td>
<td>Select this network type to isolate virtual analyzer traffic within the virtual analyzer, and when the environment has no connection to an outside network.</td>
</tr>
</tbody>
</table>

**Note:** For specified network IPv4 configuration, select an option based on your network environment. Select the manual option for direct access to the Internet.

**TABLE 6-11. Specified network options**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Analyzer port</td>
<td>Select a Virtual Analyzer port.</td>
</tr>
<tr>
<td>Note:</td>
<td>Assign a Virtual Analyzer port different from the Deep Discovery Inspector data port.</td>
</tr>
<tr>
<td>Configure IPv4</td>
<td>Select automatic configuration and click <strong>Save</strong>. STOP.</td>
</tr>
<tr>
<td></td>
<td>Select manual configuration and continue.</td>
</tr>
</tbody>
</table>
TABLE 6-11. Specified network options

<table>
<thead>
<tr>
<th>OPTION</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Address</td>
<td>Type the specific IPv4 address.</td>
</tr>
<tr>
<td>Manual configuration only</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Type the subnet mask.</td>
</tr>
<tr>
<td>Manual configuration only</td>
<td></td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Type the default gateway.</td>
</tr>
<tr>
<td>Manual configuration only</td>
<td></td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>Type the DNS server.</td>
</tr>
<tr>
<td>Manual configuration only</td>
<td></td>
</tr>
<tr>
<td>DNS Server 2</td>
<td>Type the DNS server and click Save.</td>
</tr>
<tr>
<td>Manual configuration only</td>
<td></td>
</tr>
</tbody>
</table>

b. For External Analyzer:

**Note:** The external analyzer (Deep Discovery Advisor) has more analysis capability than the internal analyzer (Virtual Analyzer).

i. Select a Virtual Analyzer IP address and API Key.

4. Select a file type.

**Note:** Highly suspicious files is the default.

a. For customized file types, either use the default selections or add/remove file types.
5. Select a maximum file size.

**Note:** Changing this setting may affect Deep Discovery Inspector performance.

6. Enable GRID analysis.

**Note:** GRID (Goodware Resource and Information Database) is a Trend Micro list of known good files, codes, and URLs. It is used to differentiate files that are safe from those that aren't. Enabling this option allows selected files to be scanned and classified prior to being submitted to the Virtual Analyzer.

7. To restore default settings, click **Restore Default**.

8. Click **Save**.

**Appliance IP Settings**

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

See **Network Interface Settings** on page 5-6 for details on configuring a dynamic IP address, and managing network interface ports.
Chapter 7

Viewing and Analyzing Information

This chapter includes information about viewing and evaluating security risks identified by Deep Discovery Inspector.

The topics discussed in this chapter are:

- Dashboard on page 7-2
- Detections on page 7-38
- Logs on page 7-55
- Reports on page 7-66
Dashboard

The Deep Discovery Inspector Dashboard displays system data, status, data analysis and statistics, along with summary graphs, based on customizable user-selected widgets.

The dashboard also contains an indicator for the amount of network traffic scanned by Deep Discovery Inspector.

**Figure 7-1.** Deep Discovery Inspector Dashboard after Initial Login
Widgets

Deep Discovery Inspector includes the following widgets:

**TABLE 7-1. Widget Types**

<table>
<thead>
<tr>
<th>Widget Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Analyzer Widgets</strong></td>
<td></td>
</tr>
<tr>
<td>Top Affected Hosts</td>
<td>This widget displays the most affected hosts within past 1 hour/24 hours/7 days/30 day as analyzed by Deep Discovery Inspector’s virtual analyzer.</td>
</tr>
<tr>
<td>Top Malicious Sites</td>
<td>This widget displays the most malicious sites within past 1 hour/24 hours/7 days/30 day as analyzed by Deep Discovery Inspector’s virtual analyzer.</td>
</tr>
<tr>
<td>Top Suspicious Files</td>
<td>This widget displays the top suspicious files within past 1 hour/24 hours/7 days/30 day as analyzed by Deep Discovery Inspector’s virtual analyzer, along with the following information: 1. The file count as detected by Deep Discovery Inspector. 2. The hosts affected by the suspicious file.</td>
</tr>
<tr>
<td><strong>Real-time Monitoring Widgets</strong></td>
<td></td>
</tr>
<tr>
<td>Monitored Network Alerts</td>
<td>This widget displays any host affected by threats within the past 24 hours. Each affected host is presented as a small circle and is grouped with the network group it belongs to.</td>
</tr>
<tr>
<td>Malicious Network Activities</td>
<td>This widget displays real-time total and malicious traffic size.</td>
</tr>
</tbody>
</table>
Monitored Network Traffic
This widget displays the total size of network traffic across the mirrored switch in real time.

Real-time Scanned Traffic
This widget displays the traffic (both safe and threat) scanned by Deep Discovery Inspector.

Threat Geographic Map
This widget displays a graphical representation of the affected hosts on a virtual world map within the past hour/current day/past 7 days/past 30 days.

Threat Summary
This widget displays the threat count of various threat types within the past 1 hour/24 hours/7 days/30 days.

Virtual Analyzer
This widget displays threat analysis results within the past 1 hour/24 hours/7 days/30 days.

Watch List
This widget displays the origination of malware attempting access to your network and allows you to configure a watch list. The watch list shows which hosts need constant monitoring.

System Status Widgets

All Scanned Traffic
This widget displays all scanned traffic within the past 24 hours.
### TABLE 7-1. Widget Types (Continued)

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Usage</td>
<td>This widget displays real-time CPU consumption for each CPU used by Deep Discovery Inspector. The indicator color is green if CPU usage is 85% or less. It turns yellow when CPU usage is between 85% and &lt; 95%, and red if more than 95%.</td>
</tr>
<tr>
<td>Disk Usage</td>
<td>This widget displays real-time disk usage for all disks. Green indicates the amount of disk space (in GB) being used. Blue indicates the amount of available disk space (in GB).</td>
</tr>
<tr>
<td>Malicious Scanned Traffic</td>
<td>This widget displays the total traffic and malicious traffic scanned within the past 24 hours.</td>
</tr>
<tr>
<td>Memory Usage</td>
<td>This widget displays real-time memory usage. Green indicates the amount (in GB) of memory being used. Blue indicates the amount (in GB) of available memory. Memory usage information is also available on the Preconfiguration Console. For details, see <em>Preconfiguration Menu: Device Information and Status</em> on page 4-6.</td>
</tr>
</tbody>
</table>

**Top Threats Widgets**

| Top Disruptive Applications   | This widget displays the most-detected disruptive applications within the past 1 hour/24 hours/7 days/30 days.                                                                                           |
| Top Exploited Hosts           | This widget displays the most-exploited hosts within the past 1 hour/24 hours/7 days/30 days.                                                                                                             |
Widgets can be customized to give administrators a clear snapshot of network health and vulnerabilities. For details, see *Customizing the Dashboard* on page 7-37.

### Displaying System Threat Data

Deep Discovery Inspector allows administrators to customize system threat data displayed on various tabs. The default tabs include:

<table>
<thead>
<tr>
<th>Widget Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Grayware-infected Hosts</td>
<td>This widget displays the most grayware-infected hosts within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Hosts with Events Detected</td>
<td>This widget displays hosts which triggered most events within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Malicious Content Detected</td>
<td>This widget displays the most-detected threats within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Malware-infected Hosts</td>
<td>This widget displays the hosts most affected by the malware within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Suspicious Behaviors Detected</td>
<td>This widget displays the most-detected suspicious behaviors within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
<tr>
<td>Top Web Reputation Detected</td>
<td>This widget displays the most-detected malicious URLs within the past 1 hour/24 hours/7 days/30 days.</td>
</tr>
</tbody>
</table>
Viewing and Analyzing Information

Threat Geographic Map Tab
This tab displays a graphical representation of affected hosts on a virtual world map. All affected hosts in different countries within a selected time frame (past 1 hour/current day/past 7 days/past 30 days) are displayed based on the source of malware, network or document exploits, and malicious email as well as the location of malware C&C servers. See Threat Geographic Map Tab on page 7-12.

Real-time Monitoring Tab
This tab contains widgets that display real-time threat data and is designed to assist administrators in identifying affected hosts and network threat distribution. See Real-time Monitoring Tab on page 7-14.

Virtual Analyzer Tab
This tab contains widgets that display the top suspicious files, top affected hosts, and top malicious sites. See Virtual Analyzer Tab on page 7-22.

Top Threats Tab
This tab contains widgets that display summary information for seven predefined threat types. See Top Threats Tab on page 7-26.

System Status Tab
This tab contains widgets that display basic Deep Discovery Inspector status including: CPU usage, memory usage, disk usage along with scanned malicious traffic and total traffic within a certain time frame. See System Status Tab on page 7-34.

Deep Discovery Inspector Custom Tabs
Deep Discovery Inspector allows you to create and customize tabs in order to organize threat information in a meaningful way.

To add a tab:

PATH: DASHBOARD

1. On the Dashboard, click the "+" sign on the empty tab.
   The New Tab window appears.
2. At the **New Tab** window, type a tab title and select layout, and auto-fit option.
3. Click **Save**.

The new tab appears on the Dashboard.

**To change tab settings:**

**Path:** DASHBOARD > TAB SETTINGS

1. On the Dashboard, select a tab to be changed and click the **Tab Settings** icon.

   The Tab Settings window appears.
2. At the Tab Settings window, change tab title, layout, and auto-fit option.
3. Click Save.

The updated tab appears on the Dashboard.

To close a tab:

**PATH: DASHBOARD**

1. On the Dashboard, select a tab you wish to close and click the "X" in the top right corner of the tab.

The tab is closed and removed from view.

**Note:** Closing the tab removes it from view; it is still available for use again by selecting Tab Settings.
To move a tab:
PATH: DASHBOARD

1. On the Dashboard, hover the mouse over the tab to be moved.
2. Left-click and drag the tab to its desired location.
   The tab (and associated widgets) is moved.

To restore the Dashboard to default settings:
PATH: DASHBOARD

1. On the Dashboard, click on the Restore link.
   A warning message appears.

   ![Dashboard Restore Message](image)

   FIGURE 7-4. Dashboard Restore Message

2. To continue Restore action, click Ok.
   Any custom tabs and widgets previously created are removed; the Dashboard is restored to its default settings.

Using Widgets

The Deep Discovery Inspector Dashboard can be customized, using 24 available widgets, to provide timely and accurate system status information. To analyze detections on the Deep Discovery Inspector widgets, go to Detections on page 7-38.

There are several controls in the top right corner of each widget:
- Click the ? icon to get help information about the widget. This includes an overview of the widget, widget data, and configuration or editable options.
- Click the Refresh icon to display the latest information on the screen. Each widget view automatically refreshes.
• Click the **Edit** icon to change the title of a widget or to modify some widget-specific information such as the type of graph displayed, the time range or some datapoints.

• Most widgets have an **Export** icon. Use this to download a .csv file containing information about widget data.

For widgets that display threat data, threat types include:

**TABLE 7-2. Threat Types Affecting Results**

<table>
<thead>
<tr>
<th>THREAT TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Content</td>
<td>Displays file signature detections.</td>
</tr>
<tr>
<td>Malicious Behavior</td>
<td>Positively-identified malware communications, known malicious destination contacted, malicious behavioral patterns and strings that definitely indicate compromise with no further correlation needed.</td>
</tr>
<tr>
<td>Suspicious Behavior</td>
<td>Anomalous behavior, false or misleading data, suspicious and malicious behavioral patterns and strings that could indicate compromise but needs further correlation to confirm.</td>
</tr>
<tr>
<td>Exploits</td>
<td>Network and file-based attempts to access information.</td>
</tr>
<tr>
<td>Grayware</td>
<td>Adware/grayware detections of all types and confidence levels.</td>
</tr>
<tr>
<td>Web Reputation</td>
<td>Malicious URLs detected.</td>
</tr>
<tr>
<td>Disruptive Applications</td>
<td>Instant messaging, streaming media, and peer-to-peer applications are considered to be disruptive because they slow down the network, are a security risk, and can be a distraction to employees.</td>
</tr>
</tbody>
</table>

Widget options are divided into five categories and are displayed on corresponding tabs:

• Threat Geographic Map
• Real-time Monitoring
• Virtual Analyzer
Deep Discovery Inspector widgets are designed to provide an overview of threats affecting your network. They include:

**Threat Geographic Map Tab**

This tab displays the Threat Geographic Map widget, a graphical representation of affected hosts on a virtual world map. All affected hosts in different countries within a selected time frame are displayed based on these five questions:

- Malware sources
- Network exploits sources
- Document exploits sources
- Malicious email sources
- Malware call-back (C&C) destinations

The Threat Geographic Map displays regions with affected hosts as a solid red circle and the Deep Discovery Inspector location being analyzed as a concentric red circle.

**FIGURE 7-5. Threat Geographic Map Widget**

*Note:* The larger the circle, the more threats have been identified.
To view information on the Threat Geographic Map:

1. Modify the time frame.
   a. Using the dropdown menu, select a tomfooleries (Past 1 hour/Today/Past 7 days/Past 30 days).

2. Modify the location.
   a. On the Threat Geographic Map, click the Edit icon.
      An edit screen appears.
   b. On the edit screen, select a location.
   c. Click Apply.
      The Threat Geographic Map is updated to reflect the new location.

3. Click any location to display relevant information in a pop-up window. See Figure 7-6.

4. Click any threat in the pop-up window.
   A table appears with details about a specific data point.

5. Click the total number of threats located at the bottom of the pop-up.
   A table populated with details about all threats (related to the indicated threat and the country or city selected) appears.
Note: The right pane displays information about affected hosts organized by country.

6. Click any country in the list to display relevant information.
7. Click **View Cities** in the pop-up window.
8. City-specific information is generated.
9. Click **View Countries** in the pop-up to return to the country list.

**Real-time Monitoring Tab**

Real-time Monitoring displays threat summary data for a certain time frame. Real-time threat data can be used to obtain an overview of threats affecting the network and which network has the most affected hosts. Seven Deep Discovery Inspector widgets are designed to give you graphical overview of threat data. They include:

**Monitored Network Alerts**

![Monitored Network Alerts Widget](image)

This widget displays all threats affecting network hosts within a 24-hour period as a circle, grouped within its network. The size of the circle represents the total number of threats. Hovering over a circle displays recent threat events. High-risk hosts are highlighted in red.

Clicking a circle displays a pop-up with additional threat information for either the past 24 hours or 30 days. Threat totals are shown for: Malicious Content, Malicious Behaviors, Suspicious Behaviors, Exploits, Grayware, along with Web Reputation and Disruptive Applications (if selected). See **Table 7-2**.
Malicious Network Activities

**FIGURE 7-8. Malicious Network Activities Widget**

This widget displays all malicious traffic detected by Deep Discovery Inspector, in a line graph format, filtered by traffic type:

- All Traffic
- HTTP
- SMTP
- Other

Traffic size is displayed with the time scale moving from right to left in seconds. Hover over a point on the graph to learn about the traffic size.

Click **Edit** to control whether data is displayed using traffic size or percent. You can also choose whether to display all scanned traffic data.
Monitored Network Traffic

![Monitored Network Traffic Widget](image)

**FIGURE 7-9.** Monitored Network Traffic Widget

This widget displays total traffic monitored by Deep Discovery Inspector, in a line graph based on all real-time HTTP, SMTP, or other traffic information. The time scale moves from right to left in seconds. Hover over a point on the graph to learn about the traffic size.

Real-time Scanned Traffic

![Real-time Scanned Traffic Widget](image)

**FIGURE 7-10.** Real-time Scanned Traffic Widget

This widget displays all real-time scanned traffic in a line graph based on all real-time HTTP, SMTP, or other traffic information. The time scale moves from right to left in seconds. Hover over a point on the graph to learn about the traffic size.
Threat Summary

FIGURE 7-11. Threat Summary Widget

This widget displays total threats within the past 24 hours, 7 days, or 30 days. Information is displayed in a graph relating time and total threats. The type of threat is distinguishable by color.

The time range is editable from the top left dropdown.

Click **Edit** to filter the types of threats displayed in the graph.

Watch List

FIGURE 7-12. Watch List Widget

The widget’s left pane contains two tabs: **Watch List** and **High Risk Hosts**. Each tab contains a list of hosts. Click a host in either tab to investigate the threats on that host. See *To investigate threats:* on page 7-19.
To view high risk host data:

The **High Risk Hosts** tab shows all high risk hosts, in the last 7 days, and can be sorted by IP address, hostname, event total, and last detected event time.

Click the plus icon to view high risk host data.

![Viewing High Risk Hosts](image1.png)

**FIGURE 7-13.** Viewing High Risk Hosts

To add hosts to the Watch List:

If a host requires additional monitoring add it to the **Watch List** tab.

1. Type the host’s full IP address in the search text box (a partial IP address is not accepted).
   
   A field containing the IP address appears.

   ![Adding Hosts to the Watch List](image2.png)

   **FIGURE 7-14.** Adding Hosts to the Watch List

2. In the IP address (Configuration) field, type a note for that host and click **Save & Watch**.
To edit the Watch List:

1. Sort the Watch List by desired criteria.
2. Click the plus icon for the host to be edited.

![Edit Watch List]

**FIGURE 7-15. Edit Watch List**

3. Edit the note for this hosts and click **Save & Watch**.
4. Remove hosts from the Watch List, click the tool icon and select Remove.

![Remove Hosts from Watch List]

**FIGURE 7-16. Remove Hosts from Watch List**

To investigate threats:

1. Go to either the **Watch List** or **High Risk Hosts** tab and click on the host to be investigated.
   
   The time-series line graph to the right plot is populated with the threat count on
   that host by threat type and for a particular time period (past 24 hours, 7 days, and
   30 days).
Note: Threat types include known malware, malicious behavior, suspicious behavior, exploit, and grayware. See Table 7-2 for threat descriptions. For known malware and exploits, all detections are counted in the graph. For malicious behavior, suspicious behavior, and grayware, only those that are considered high risk are displayed in the graph.

Tip: If you choose Past 24 hours and the current time is 4:15pm, the graph shows the threat count for each threat type from 5:00pm of the previous day to 4:00pm of the current day.

2. Click a data point in the graph.

The Detection screen with detailed threat information opens.

Virtual Analyzer

![Virtual Analyzer Widget](image)

**FIGURE 7-17. Virtual Analyzer Widget**
To view analysis results:

1. Select a time period (Past 1 hour, Past 24 hours, Past 7 days, Past 30 days).

   **Note:** The Virtual Analyzer must be enabled in order to view results.

2. Hover over a section of the chart to view the percentage of Malicious or Not Malicious analyzed files.

3. View Virtual Analyzer status on the left pane.
   a. For Virtual Analyzer:
      - Analysis Module: Internal
      - Virtual Analyzer Status: Enabled
      - OS Version: for the imported image
      - Last File analyzed: last scanned file name or SHA-1
      - Last file analysis date:
      - Virtual Analyzer import date:
      - # of files to be analyzed:
      - Average analysis time per file:
      - Cache hit rate:

   b. For Deep Discovery Advisor:
      - Analysis Module: Deep Discovery Advisor
      - Last File analyzed: last scanned file name or SHA-1
      - Last file analysis date:
      - # of files to be analyzed:
      - Average analysis time per file:
      - Cache hit rate:
Virtual Analyzer Tab

Advanced Persistent Threats (APT) are targeted attacks with a pre-determined objective: steal sensitive data or cause targeted damage. The objective is not the defining attribute of this type of attack; it’s the fact that attackers are persistent in achieving their objective. See Virtual Analyzer Widgets Data on page 7-22 for information about the data displayed.

### TABLE 7.3. Virtual Analyzer Widgets Data

<table>
<thead>
<tr>
<th>DATA</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detections</td>
<td>An event detected by Deep Discovery Inspector within a certain time frame.</td>
</tr>
<tr>
<td>Affected hosts</td>
<td>Any host that was affected by a threat. Information about the threat can be downloaded for further analysis.</td>
</tr>
</tbody>
</table>

Deep Discovery Inspector widgets are designed to show any Advanced Persistent Threats detected by Deep Discovery Inspector and analyzed by Virtual Analyzer. They include:

- Top Affected Hosts
- Top Malicious Sites
- Top Suspicious Files

Using this summary data gives administrators insight into what type of threat file types are affecting the network, which hosts are affected, and which malicious sites are attempting network access.
Top Affected Hosts

This widget displays the top affected hosts as analyzed by Virtual Analyzer (internal analyzer as detections per IP address).

Viewing hosts attacked in the past 1 hour, 24 hours, 7 days, or 30 days and the type of detected attack allows users (typically system or network administrators) to take appropriate action (blocking network access, isolating computers according to IP address) in order to prevent malicious operations from affecting hosts.

Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number of affected hosts displayed (up to 20).
Top Malicious Sites

FIGURE 7-19.  Top Malicious Sites Widget

This widget displays the top malicious sites analyzed by Virtual Analyzer (internal analyzer) as detections per affected host. Deep Discovery Inspector, combined with Trend Micro Smart Protect Service, queries the level of security of destinations.

Viewing the top malicious sites mounting attacks against system hosts within the past 1 hour, 24 hours/7 days/30 days allows users (typically system or network administrators) to take appropriate action (blocking network access to these malicious destinations by proxy or DNS server) in order to prevent malicious operations from affecting hosts.

All malicious sites within a chosen time frame are shown in a chart. Click any cell to obtain additional details about the site.
Top Suspicious Files

**FIGURE 7-20. Top Suspicious Files Widget**

This widget displays top suspicious files (attached to HTTP traffic, FTP traffic or email) as analyzed by Virtual Analyzer, along with the following information:

- The file count as detected by Deep Discovery Inspector
- The hosts affected by the suspicious file.

Viewing suspicious files affecting hosts within the past 1 hour, 24 hours, 7 days or 30 days in a graphical format allows users (typically system or network administrators) to take appropriate action by adding email block lists, changing HTTP or FTP servers, modifying system files, or writing registry keys) in order to remove malicious operations from affecting hosts.

Data gathered about the affected hosts includes:

**TABLE 7-4. Top Suspicious Files Data**

<table>
<thead>
<tr>
<th>COLUMN NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name/SHA-1</td>
<td>The suspicious file name.</td>
</tr>
<tr>
<td>Detections</td>
<td>Any event detected by Deep Discovery Inspector within a certain time frame.</td>
</tr>
<tr>
<td>Affected Hosts</td>
<td>Any host that was affected by a suspicious file.</td>
</tr>
<tr>
<td>Malware Name</td>
<td>The name of the known malware.</td>
</tr>
<tr>
<td>Severity</td>
<td>The level of threat by suspicious files.</td>
</tr>
</tbody>
</table>
Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number of top suspicious files displayed (up to 20).

**Top Threats Tab**

The Top Threats tab displays threat summary information from various perspectives. Administrators can use top threats data to identify the most dangerous hosts or the most severe threats in order to take appropriate action. Eight Deep Discovery Inspector widgets are designed to identify the most affected hosts along with the most severe threats within certain time frames. For each widget, a detailed threat log can be exported for further analysis.

**Top Disruptive Applications**

![Top Disruptive Applications Widget](image)

**FIGURE 7-21. Top Disruptive Applications Widget**

This widget displays disruptive application threats within the past 1 hour, 24 hours, 7 days, or 30 days. For a description of disruptive applications, see *Table 7-2*. Clicking on a table cell provides additional details.

Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number of top disruptive applications displayed (up to 20).
Top Exploited Hosts

This widget shows which hosts on your network(s) have been most affected by exploit attempts within the past 1 hour, 24 hours, 7 days, or 30 days. For a description of exploits, see Table 7-2. By default, all exploited hosts within the selected time frame are shown in a bar graph relating the IP addresses of the top exploited hosts and total detections.

Mouse over an area on the graph to see the exact number of exploits on a host. Clicking this point will open a detection list with details about the type and severity of a threat, the hostname, the timestamps, and the total detected exploits.

Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number to exploited hosts displayed (up to 20).
Top Grayware-infected Hosts

This widget displays the most detected grayware on your network(s) within the past 1 hour, 24 hours, 7 days, or 30 days. For a description of grayware, see Table 7-2.

**Note:** This widget shows only those hosts with threats categorized as "High" severity.

By default, all known malware detections within the selected time frame are shown in a pie chart. Mouseover an area to see the name of the top grayware-infected hosts. Clicking this point opens a detection list with details about the date, type, source/destination IP, protocol, direction or file name.

Click **Edit** to change whether data is displayed in a chart, graph or table. You can also control the total number of grayware-infected hosts displayed (up to 20).
Top Hosts with Events Detected

This widget displays events affecting hosts within the past 1 hour, 24 hours, 7 days, or 30 days. By default, all events within the selected time frame are shown in a bar graph relating the IP addresses of the top exploited hosts and total detections.

Mouseover an area on the graph to see the exact number of hosts with events detected. Clicking this point opens a detection list with details about the severity and type of threat, the hostname, the timestamps, and the total detections.

Click Edit to change whether data is displayed in a chart, graph or table. You can also control the total number to hosts displayed (up to 20).
Top Malicious Content Detected

This widget displays the most-detected known malware on your network(s) within the past 1 hour, 24 hours, 7 days, or 30 days. For a description of known malware, see Table 7-2.

By default, all known malware detections within the selected time frame are shown in a pie chart. Mouseover an area to see the name of the malware detected on a host. Clicking the malware name opens a detection list with details about the date, type, source/destination IP, protocol, direction or file name.

Click Edit to change whether data is displayed in a chart, graph or table. You can also control the total number of exploited hosts displayed (up to 20).
Top Malware-infected Hosts

This widget displays the most malware-infected hosts on your network(s) within the past 1 hour, 24 hours, 7 days, or 30 days. For a description of malware, see Table 7-2.

By default, all malware-infected hosts within the selected time frame are shown in a bar graph relating the IP addresses of the infected hosts and total detections.

Mouseover an area on the graph to see the exact number of malware-infected hosts. Clicking this point opens a detection list with details about the type and severity of a threat, the hostname, the timestamps, and the total detected infections.

Click Edit to change whether data is displayed in a chart, graph or table. You can also control the total number to malware-infected hosts displayed (up to 20).
Top Suspicious Behaviors Detected

This widget displays the most detected suspicious behavior on your network(s) within the past 1 hour, 24 hours, 7 days, or 30 days. For a description of suspicious behavior, see Table 7-2.

Note: This widget shows only those hosts with behavior categorized as "High" severity.

Click Edit to change whether data is displayed in a chart, graph or table. You can also control the total number to suspicious behaviors displayed (up to 20).
Top Web Reputation Detected

This widget displays the most web reputation detections within the past 1 hour, 24 hours, 7 days, or 30 days. For a description of web reputation, see Table 7-2.

By default, all detections within the selected time frame are shown in a table relating URL and total detections. Clicking any data point opens a detection list with details about the threat, timestamp, source/destination IP, and the malicious URL hostname.

Click Edit to change whether data is displayed in a chart, graph or table. You can also control the total number to hosts displayed (up to 20).
System Status Tab

System Status tells administrators whether Deep Discovery Inspector is operating within specifications; insufficient resources may cause a system failure. These widgets display real-time system resource data to ensure that all Deep Discovery Inspector resources are operating within specifications. Five widgets are designed to display system resource usage and traffic scanned by Deep Discovery Inspector within the past 24 hours.

All Scanned Traffic

This widget displays all scanned traffic for the past 24 hours and can be filtered by traffic type:

- All traffic
- HTTP
- SMTP
- Other
CPU Usage

![CPU Usage Widget](image)

**FIGURE 7-30. CPU Usage Widget**

This widget displays what percent of each CPU is being used.

Disk Usage

![Disk Usage Widget](image)

**FIGURE 7-31. Disk Usage Widget**

This widget displays how much disk space is available for your appliance.
Malicious Scanned Traffic

This widget displays malicious traffic as a subset of all scanned traffic, in a line graph format, for a 24-hour time period. This data can be filtered by traffic type:
- All traffic
- HTTP
- SMTP
- Other

Memory Usage

This widget displays how much memory is available on your appliance.
Customizing the Dashboard

Deep Discovery Inspector widgets can be added and removed from view, as needed, to customize your Deep Discovery Inspector interface.

To add a widget:

**PATH: DASHBOARD > ADD WIDGET**

1. On the Dashboard, click the **Add Widgets** icon. The **Add Widgets** screen appears.

![Add Widgets Screen](image)

**FIGURE 7-34. Add Widgets Screen**

2. At the **Add Widgets** Screen, select which widgets to display in each tab.
3. Click **Add**. The selected widget(s) appear on the Dashboard.

To close a widget:

**PATH: DASHBOARD**

1. Select a tab on the Dashboard that displays the widget you wish to close.
2. Click the "X" at the top right corner of the widget display.

**Note:** Closing the widget removes it from the tab; it is still available for use again by selecting **Add Widget**.

To move a widget:

**PATH: DASHBOARD**

1. Select a tab on the Dashboard that displays the widget you wish to move.
2. Hover the mouse over the widget title bar until a four-headed arrow appears.
3. Left-click the mouse and drag the widget to its desired location within the tab.
Detections

The Detections tab contains a list of hosts experiencing an event (threat behavior with potential security risks, known threats, or malware) for a past 1 hour, 24-hour, 7-day, or 30-day time period. Deep Discovery Inspector tags these events as security risks/threats and makes a copy of the files for assessment.

Clicking on any column title sorts that column in either ascending or descending order. To view detection details, click any of the links within the table.

Data shown on the Detections window is aggregated from raw log data every 10 minutes.

FIGURE 7-35. Detections Window
### TABLE 7-5. Detections window columns

<table>
<thead>
<tr>
<th>TABLE COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latest Detection</td>
<td>Most recent detection, based on time stamp</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the affected host</td>
</tr>
<tr>
<td>Hostname</td>
<td>Name of the affected host</td>
</tr>
<tr>
<td>Group</td>
<td>Network group to which an host's IP address belongs. Go to Administration &gt; Network Configuration &gt; Monitored Network to monitor a host’s IP address.</td>
</tr>
<tr>
<td>Real-time Detections</td>
<td>Expanding this link, allows the user to view the total detections for all types of threats. See Threat Types Affecting Results.</td>
</tr>
<tr>
<td>Correlated Incidents</td>
<td>The number of the incidents which match the deep correlation rule.</td>
</tr>
<tr>
<td>Virtual Analyzer Detections</td>
<td>The total number of virtual analysis detections.</td>
</tr>
</tbody>
</table>
Detection Details

Deep Discovery Inspector logs the details of each Internet threat it identifies.

To searching for hostname or IP addresses:

**PATH:** DETECTIONS

1. Type a hostname or IP address in the search field and click the Search button. The requested information is displayed.

![Search hostname or IP address](image)

**FIGURE 7-36.** Detections Screen Search Function

2. Click Clear Search to return to the Detections screen.

To change the time range:

**PATH:** DETECTIONS

Select a time range for which to view threat data. Data is sorted based on selection.

![Time Range Selector](image)

**FIGURE 7-37.** Time Range Selector

To export .csv files:

**PATH:** DETECTIONS > EXPORT ICON

1. Click the Export icon.
   
   A File Download window appears.

2. Select whether to Open or Save (recommended) the Threat_Detections.csv file and click the corresponding button.
   
   The Threat_Detections.csv file is saved as an .xls spreadsheet.

**Note:** Select the Open option to view the file. Select the Save option to store the file for future reference and analysis.
To customize columns:
PATH: DETECTIONS > CUSTOMIZE COLUMNS ICON

1. Click the Customize columns icon.
   A column title window appears.
2. On the column title window select which items to include in the Detections table.
3. Click Save.
   The Detections table column title window appears.

To search data by page:
PATH: DETECTIONS

1. Select a page to view by typing the page number in the Page: field.
2. Select the number of entries per page (25, 50, or 100).
3. Data is sorted based on selection.

To view Real-time Detections Details:
PATH: DETECTIONS

1. Click the double arrow next to Real-time Detections.
   A list of real-time detections appears.

   ![Real-time Detections List](image)

   **FIGURE 7-38. Real-time Detections List**

Note: Real-time detections include: Malicious Content, Malicious Behavior, Suspicious Behavior, Exploits, Grayware, Web Reputation, and Disruptive Applications.

2. On the real-time detections list, click a link under the Real-time Detections column, to view all current real-time threats.
   The total real-time detections list appears.
7-42

FIGURE 7-39. Total Real-time Detections List

a. Select a column name to sort the results.

b. Click Export icon to save the results to a file.

c. Click Mark all as resolved when the risk has been eliminated from the host.

See Mitigation Device Settings starting on page 6-36,

The number of Unresolved Detections changes.

3. At the total real-time detections list, click on the Total Detections link to view detection details.

FIGURE 7-40. Detections Details Screen

4. Click on the Other Hosts tab to view other hosts affected by the same threat.
At the Detection Details screen, click on threat name link to view the latest information on this threat.

Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.

The Threat Connect results screen appears with a message alerting user whether a match is found or not.
When a match is found, review the information provided.
If a match is not found, review the on-screen instructions.

To view Correlated Incidents Detection Details

**PATH:** Detections

1. On the Detections page, click any Correlated Incidents link.
A list of correlated incidents opens.
2. At the correlated incidents list, click on the Total Incidents link. The Detection Details screen appears.

![Detection Details Screen](image)

**FIGURE 7-44. Correlation Incidents Detection Details**

3. At the Detection Details screen, click on threat name link to view the latest information on this threat.

Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.

The Threat Connect results screen appears with a message alerting user whether a match is found or not.
When a match is found, review the information provided.

b. If a match is not found, review the on-screen instructions.

To view Virtual Analysis Detection Details

1. On the Detections page, click any Virtual Analysis Detections link. A list of virtual analysis detections opens.

2. Click on Total Detections link to view detection details. The Detection Details screen appears.
3. At the Detection Details screen, click on threat name link to view the latest information on this threat.

   Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.

   The Threat Connect results screen appears with a message alerting user whether a match is found or not.
When a match is found, review the information provided.

If a match is not found, review the on-screen instructions.

**To view Malicious Content Details:**

**PATH: DETECTIONS**

1. Click on Malicious Content link.
   A malicious content detections list opens.
2. Click the link in the Total Detections column to view detection details.
   The Detection Details screen appears.

**FIGURE 7-49. Malicious Content Details Screen**

1. Click the Other Hosts tab to view other hosts affected by the same threat.
2. At the Detection Details screen, click on threat name link to view the latest information on this threat.

Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.

The Threat Connect results screen appears with a message alerting user whether a match is found or not.
When a match is found, review the information provided.
If a match is not found, review the on-screen instructions.

**To view Malicious Behavior details:**

**PATH: Detections**

1. Click on Malicious Behavior link.
   A malicious behavior detections list opens.
2. Click the link in the Total Detections column to view detection details.

![Malicious Behavior Details Screen](image)

**FIGURE 7-50. Malicious Behavior Details Screen**

3. Click the Other Hosts tab to view other hosts affected by the same threat.
4. At the Detection Details screen, click on threat name link to view the latest information on this threat.

   Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.

   The Threat Connect results screen appears with a message alerting user whether a match is found or not.

   a. When a match is found, review the information provided.
   b. If a match is not found, review the on-screen instructions.
To view Suspicious Behavior details:

**PATH: DETECTIONS**

1. Click on Suspicious Behavior link.
   
   A suspicious behavior detections list opens.
2. Click the link in the Total Detections column to view time-based detections data.

**FIGURE 7-51. Suspicious Behavior Details Screen**

3. Click on the Other Hosts tab to view other hosts affected by the same threat.
4. At the Detection Details screen, click on threat name link to view the latest information on this threat.
   
   The Threat Connect Summary screen appears.

   Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.

   The Threat Connect results screen appears with a message alerting user whether a match is found or not.
   
   a. When a match is found, review the information provided.
   
   b. If a match is not found, review the on-screen instructions.
To view Exploit details:
PATH: Detections > Detections List

1. Click on Exploit link.
   An exploit detections list opens.
2. Click the link in the Total Detections column to view time-based data.

3. Click on the Other Hosts tab to view other hosts affected by the same threat.
4. At the Detection Details screen, click on threat name link to view the latest information on this threat.
   Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.
   The Threat Connect results screen appears with a message alerting user whether a match is found or not.
   a. When a match is found, review the information provided.
   b. If a match is not found, review the on-screen instructions.
To view Grayware details:

**PATH:** Detections > Detections List

1. Click on Grayware link.
   A grayware detections list opens.
2. Click the link in the Total Detections column to view detection details.

![Grayware Details Screen](image)

**FIGURE 7-53. Grayware Details Screen**

3. Click on the Other Hosts tab to view other hosts affected by the same threat.
4. At the Detection Details screen, click on threat name link to view the latest information on this threat.

Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.

The Threat Connect results screen appears with a message alerting user whether a match is found or not.

- When a match is found, review the information provided.
- If a match is not found, review the on-screen instructions.
To view Web Reputation details:

**PATH: DETECTIONS > DETECTIONS LIST**

1. Click on Web Reputation link.
   A web reputation detections list opens.
2. At the Detections List window, click the link in the Total Detections column to view time-based data.

![Web Reputation Details Screen](image)

**FIGURE 7-54.** Web Reputation Details Screen

3. Click on the Other Hosts tab to view other hosts affected by the same threat.
4. At the Detection Details screen, click on threat name link to view the latest information on this threat.
   Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.
   The Threat Connect results screen appears with a message alerting user whether a match is found or not.
   a. When a match is found, review the information provided.
   b. If a match is not found, review the on-screen instructions.
To view Disruptive Applications details:

**Path:** **Detections > Detections List**

1. Click on Disruptive Applications link.
   A disruptive application detections list opens.
2. At the Detection List window, click the link in the Total Detections column to view time-based data.

**FIGURE 7-55. Disruptive Applications Details Screen**

3. Click on the Other Hosts tab to view other hosts affected by the same threat.
4. At the Detection Details screen, click on threat name link to view the latest information on this threat.
   Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.
   The Threat Connect results screen appears with a message alerting user whether a match is found or not.
   a. When a match is found, review the information provided.
   b. If a match is not found, review the on-screen instructions.
Logs

Deep Discovery Inspector maintains comprehensive logs about security risk incidents, events, and updates. Queries can be used to gather information and create reports from the log database.

These logs are stored in the Deep Discovery Inspector database, in the Trend Micro Control Manager (TMCM) database, or on a Syslog server.

Types of log queries include:

<table>
<thead>
<tr>
<th>TABLE 7-6. Log types</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TYPE</strong></td>
</tr>
<tr>
<td>Detection Logs Query</td>
</tr>
<tr>
<td>System Logs Query</td>
</tr>
</tbody>
</table>

Detection Logs Query

When Deep Discovery Inspector scans the network and detects a threat, it collects the results of the scan, and the status of the scanned hosts, and creates a Detections Log. If Deep Discovery Inspector is registered to Control Manager, Control Manager stores the scan results received from Deep Discovery Inspector.

Detection logs can be queried by setting query criteria. Use queries to obtain information from these logs.
To query detections:

**PATH:** 
Logs > Detections Log Query

**FIGURE 7-56. Detections Logs Query**

Adjust the following **Criteria** as needed:

1. Specify a **Time range** or click the calendar icon to select a specific date.
2. Select the **Endpoint**.
   
   c. Check **All Computers**.
   
   d. *(Optional)* Select **Computer name, AD domain or account, and/or MAC address**.

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

3. *(Optional)* Select **IP address** or a range of IP addresses.
f. (Optional) Select the **Groups**.

**TABLE 7-7. Group name options**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>Select from one of the group names in the list.</td>
</tr>
<tr>
<td>All groups</td>
<td>Uses default settings to select all groups.</td>
</tr>
<tr>
<td>Not in group</td>
<td>Select this option for groups that do not fall under any of the other categories.</td>
</tr>
<tr>
<td>Removed group</td>
<td>Select this option if the group name is not available in the list, if the exact name is not known, or if the group name has been deleted.</td>
</tr>
</tbody>
</table>

3. Select **Detection Type**.

**TABLE 7-8. Detection Type Options**

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats</td>
<td>Select this option to generate logs about all unwanted access to information from Malicious Content, Grayware, Exploits, Malicious Behavior, and/or Suspicious Behavior. Choose the Types, Severity, Malware Name, Protocol, Directions, Network Zone, Mitigation, Outbreak Containment Service, and/or Detection Files to customize the threat log query.</td>
</tr>
</tbody>
</table>
4. Click **Search** to run the Detections Log Query.
   The Detections Log Query results screen appears.

### TABLE 7-8. Detection Type Options

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disruptive Applications</td>
<td>Select this option to generate logs about any peer-to-peer, instant messaging, or streaming media applications considered to be disruptive because they slow down the network, are a security risk, and are generally a distraction to employees. Choose <strong>Protocol</strong> and <strong>Directions</strong> to customize the disruptive application log query.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Select <strong>Internal detection</strong> of to view in-network IP address sources.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Select <strong>External detection</strong> to view out-of-network IP address sources.</td>
</tr>
<tr>
<td>Malicious URL</td>
<td>Select this option to generate logs about all websites that try to perform malicious activities. Malicious URL includes Trojan Horse programs, spyware, adware, Pharming and other malware.</td>
</tr>
<tr>
<td>Virtual Analysis</td>
<td>Select this option to generate logs about files analyzed by the virtual analyzer. Select the threat severity and, if needed, the file name and SHA-1 name. Choose <strong>Severity</strong>, <strong>File Name</strong> (optional) and <strong>SHA-1</strong> (optional) to customize the Virtual Analysis log query.</td>
</tr>
<tr>
<td>Correlated Incidents</td>
<td>Select this option to generate logs about correlated incidents. Choose <strong>Severity</strong>, <strong>Correlation Rule ID (ICID)</strong> (optional), <strong>Incident Name</strong> (optional), and <strong>Protocol</strong> to customize the Correlated Incident log query.</td>
</tr>
</tbody>
</table>
Viewing and Analyzing Information

**FIGURE 7-57.** Detections Log Query Results - Threats

**FIGURE 7-58.** Detections Log Query Results - Disruptive Applications
### FIGURE 7-59. Detections Log Query Results - Malicious URL

![Malicious URL Detections Log Query](image1)

### FIGURE 7-60. Detections Log Query Results - Virtual Analysis

![Virtual Analysis Detections Log Query](image2)

### FIGURE 7-61. Detections Log Query Results - Correlated Incidents

![Correlated Incidents Detections Log Query](image3)
5. To start a new query, click the Start new query icon.

Note: Do not use the browser's back button the start a new query. Using the browser's back button returns user to the Deep Discovery Inspector Dashboard.

6. Obtain additional details about detections on the log, as needed. See Detection Log Query Details.

7. Click Export to export the detections log to a .CSV file, as needed.

Detection Log Query Details

Deep Discovery Inspector logs the details of each threat it identifies. The Detection Log Query Details screen on the product console may contain any of the following information, depending on the protocol, file and other factors:

To view detection log query details:

Path: Detections Log Query Results

1. On the detections log query results screen, click on the Date link.

   The Detection Details screen appears, divided into two sections:
   - Header
     name
     severity
     type
   - Connections Details (based on search criteria) may include:
     Detection direction
     Host
     Protocol Details
     File Details
     Additional Event Details
2. On the Detections Detail screen, click on the **Detection Name** link.

Deep Discovery Inspector connects with Threat Connect to search thousands of reports to provide details about detected threat behavior.

The Threat Connect results screen appears with a message alerting user whether a match is found or not.

a. When a match is found, review the information provided.

b. If a match is not found, review the on-screen instructions.
### Protocol Details

#### TABLE 7-9.  Event details for traffic through various protocols

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

### File Details

#### TABLE 7-10.  File details

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>Name of the file tagged as a potential/known risk</td>
</tr>
<tr>
<td>File size</td>
<td>Size of the file tagged as a potential/known risk</td>
</tr>
<tr>
<td>File extension</td>
<td>Extension of the file tagged as potential/known risk</td>
</tr>
<tr>
<td>File name in archive</td>
<td>Name of the file in the archive tagged as potential/known risk</td>
</tr>
</tbody>
</table>
Additional Event Details

TABLE 7-11. Additional event details

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Whether the protocol requires authentication</td>
</tr>
<tr>
<td>URL</td>
<td>Link included in the email or the instant message content</td>
</tr>
<tr>
<td>BOT command</td>
<td>Command used in IRC for BOTs</td>
</tr>
<tr>
<td>BOT URL</td>
<td>URL used in IRC for BOTs</td>
</tr>
<tr>
<td>Intelligent Rule ID</td>
<td>Defined in Network Content Correlation Pattern, used by the Network Content Correlation Engine</td>
</tr>
<tr>
<td>Detected by</td>
<td>Displays the engine that detected the threat (Network Content Inspection Engine, Advanced Threat Scan Engine, and/or Network Content Correlation Engine)</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used by the threat traffic</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Indicates whether any mitigation action is needed.</td>
</tr>
<tr>
<td>Outbreak Containment Services</td>
<td>Indicates if any containment services are needed, when an outbreak is detected.</td>
</tr>
</tbody>
</table>

System Logs Query

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

To query system:

PATH: LOGS > SYSTEM LOG QUERY

1. Adjust the following Criteria as needed.
   a. Specify a Time range or click the calendar icon to select a specific date.
2. Select a Log Type (All system logs, System events, or Update events)
3. Click Search to run the System Log Query.
4. Click **Export** to export the system log to a `.csv` file.

![System Log Query Results](image)

**Figure 7-63. System Log Query Results**

**Syslog Server Settings**

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

**To send logs to Syslog servers:**

**PATH:** LOGS > SYSLOG SERVER SETTINGS

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

**Using Logs**

Log query results are designed to assist the administrator determine what action to take depending on various criteria (affected host, type of threat). Use log data to manage the network environment.
Reports

Deep Discovery Inspector provides various reports to assist in mitigating threats and optimizing system settings. Reports can be scheduled for daily, weekly, and executive summary generation. The web console Reports screen contains two tabs:

- Generate Reports
- Report Notification Settings

Generated Reports

There are two types of user-generated reports:

- Scheduled Reports
- On-Demand Reports

![Generated Reports Selection Screen](image)

**FIGURE 7-64. Generated Reports Selection Screen**
Scheduled Reports
PATH: REPORTS > GENERATE REPORTS > SCHEDULED REPORTS

The Scheduled Reports tab allows user to receive reports on a regular basis.

1. On the Scheduled Reports tab click a date from which to view reports.
   The available reports are displayed.
   Calendar icons include:
   D = daily report
   W = weekly report
   M = monthly report
2. Select a report to view or save.

On-Demand Reports
PATH: REPORTS > GENERATE REPORTS > ON-DEMAND REPORTS

The On-demand tab allows user to generate reports on a real-time basis.

1. On the On-demand Reports click New.
   A New Report window opens.
2. At the New Report window, select a Report Time Range, up to 4 weeks previous.
4. Click Generate.
   A .pdf version of the requested report is generated.
5. To view the report, click on the PDF link and select Open.
6. To save the report, click on the PDF link and select Save. Alternatively, open the report and select Save As.
7. To delete a report, select it in the On-Demand Reports list and click Delete.

Report Notification Settings

To receive reports automatically, at a specified internal (Daily, Weekly, Monthly), check Notify Administrator, select the interval, and click Save.
Using Reports

Reports use forensic analysis and threat correlations to in-depth analyze Deep Discovery Inspector event logs to identify the threats more precisely. Reports are designed to assist the administrator determine the types of threat incidents affecting the network. Daily administrative reports enable IT administrators to track the status of threats, while weekly and monthly executive reports keep executives informed about the overall security posture of the organization.

Scheduled Reports

Daily, weekly, and monthly reports are designed to provide the correlated threat information. See Threat Management Services Portal on page 6-39.

Virtual Analyzer Reports

Virtual Analyzer reports are designed to provide detailed information about specific files.
Maintenance

This chapter explains how to perform maintenance tasks for Deep Discovery Inspector.

The topics discussed in this chapter are:

- *Licenses and Activation Codes* on page 8-2
- *Appliance Rescue* on page 8-3
Licenses and Activation Codes

The Product License screen displays license information and accepts valid Activation Codes for Deep Discovery Inspector.

The trial license limits some of the available on-screen information for the following widgets:

- All Scanned Traffic
- Malicious Network Activities
- Malicious Scanned Traffic
- Monitored Network Traffic
- Real-time Scanned Traffic
- Virtual Analyzer

For details, see Licenses and Activation Codes on page 5-9.

Log/Report Maintenance

Deep Discovery Inspector maintains logs and reports in the product’s hard disk. To set criteria and view logs go to Detection Logs Query on page 7-55 and System Logs Query on page 7-64. Manually delete logs and reports on a regular basis to keep them from occupying too much space on the hard disk. The deletion schedule will depend on your environment and the quantity of logs and reports to be retained.

If the disk size is not enough for log and report storage, Deep Discovery Inspector automatically deletes logs beginning with the oldest, by date. If deleting earlier logs does not provide enough disk space, Deep Discovery Inspector automatically deletes subsequent logs until the disk size is sufficient to hold the latest logs.

Note: Deep Discovery Inspector can send logs to a Syslog Server or Trend Micro Control Manager. For details, see Syslog Server Settings on page 7-65 and Control Manager Settings on page 6-43.

To configure log maintenance settings:

**PATH:** ADMINISTRATION > LOG/REPORT MAINTENANCE

1. Select which logs to delete, on the Log/Report Deletion screen.
2. Select a deletion action.
   a. Select either **Delete all logs selected above** or **Delete logs selected above older than** the specified number of days.
3. Click **Delete**.

To perform maintenance tasks for the product database:

**PATH:** ADMINISTRATION > LOG/REPORT MAINTENANCE

1. Click **Check database status**.
2. If one or more database files are corrupted, click **Repair**.
   The product repairs the corrupted files and indicates a database status when repair action is complete.

Appliance Rescue

Rescuing the software appliance means reinstalling Deep Discovery Inspector and reverting to saved or default settings. As an alternative, update the firmware to rescue the software appliance. See *Firmware Update* on page 6-32.

Use appliance rescue if Deep Discovery Inspector files become corrupted. Rescuing the software appliance reinstalls the Deep Discovery Inspector feature that monitors traffic and creates logs.

**WARNING!** Unplug external USB storage devices before continuing with appliance rescue.

**WARNING!** To prevent a rescue operation failure, detach iDRAC virtual media device before beginning the rescue operation. For additional details, see *Glossary* on page 10-1.

Rescuing the software appliance is not the same as applying a system update:
Rescuing: Replaces application files and keeps or restores the default settings.

Applying a system update: Updates the existing application files to enhance features.

**WARNING!** Before rescuing the appliance, create a backup of your settings. For details, see *Backup/Restore Appliance Configuration* on page 6-26.

**To enter rescue mode:**

**Note:** Using a monitor connected to a VGA port is the only supported method for rescue operations.

1. Log on to the Preconfiguration Console through a monitor after connecting to Deep Discovery Inspector via serial connection. For details, see *The Preconfiguration Console* on page 4-2.
2. Type 4 and press ENTER.
   The System Tasks screen appears.
3. Type 6 and press ENTER.
   The Restart System screen appears.

**FIGURE 8-1.** Restart System Screen
4. Select **OK**.
   The software appliance restarts.

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

![Escape Initiation Screen](image1)

**FIGURE 8-2.** Escape Initiation Screen

The boot menu appears.

![Boot Menu](image2)

**FIGURE 8-3.** Boot Menu
6. Type 4 and press ENTER.
   The Deep Discovery Inspector rescue mode screen appears.

7. Copy the Deep Discovery Inspector Rescue Tool (Rescue.exe) from the Solutions CD to the host.

   **WARNING!** Ensure Deep Discovery Inspector appliance is in rescue mode before using the rescue tool.

   **Note:** In rescue mode, the Deep Discovery Inspector IP address is 192.168.252.1 and the subnet mask is 255.255.255.0.

   **Note:** Ensure that the host running the rescue tool is on the same network segment (192.168.252.0/24) as Deep Discovery Inspector.

8. Double-click Rescue.exe to launch the rescue tool.
9. Browse to the latest image file: *.R.
10. Click **Update**.
The Deep Discovery Inspector Rescue Tool uploads the new image.

**Note:** Do not turn off or reset the appliance during the update process.

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

12. Type **Y** to migrate the previous configuration files.

13. Press **ENTER** to continue.

   Deep Discovery Inspector starts migrating the configuration files.

Getting Help

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

The topics discussed in this chapter are:

- Frequently Asked Questions (FAQs) on page 9-2
- Before Contacting Technical Support on page 9-7
- Contacting Trend Micro on page 9-8
Frequently Asked Questions (FAQs)

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

**Installation**

**Will the Deep Discovery Inspector installation disrupt network traffic?**

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

**Activation**

**Do I need to activate Deep Discovery Inspector after installation?**

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

**Configuration**

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

After five minutes of inactivity, Deep Discovery Inspector logs out of the inactive session.

**Can I register Deep Discovery Inspector to more than one Control Manager server?**

No, you cannot register Deep Discovery Inspector to more than one Control Manager server. To register Deep Discovery Inspector to a Control Manager server, refer to Control Manager Settings on page 6-43.

**Will changing the Deep Discovery Inspector IP address prevent it from communicating with the Control Manager server?**

Yes, changing the Deep Discovery Inspector IP address through the Preconfiguration Console or product console will cause temporary disconnection (30 seconds). During the time the Management Communication Protocol (MCP) agent is disconnected from Control Manager, the MCP agent logs off from Control Manager and then logs on to provide Control Manager with the updated information.
I typed the wrong password three times when logging on to the Preconfiguration Console. Then, I could no longer log on to the Preconfiguration Console. What should I do?

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

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

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

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

Ensure that:
- The TMSP logon details are correct.
- The firewall settings are configured to allow port 22 or 443 traffic.
- The proxy settings are correct.

If the problem persists, consult your support provider.

Do I need to reconfigure the Syslog Server settings after importing the configuration file exported from TDA 2.6 (or another previous version)?

Yes, reconfigure the Syslog Server settings after every fresh Deep Discovery Inspector installation; the configuration file cannot be imported from previous versions.

What can I do when the email notification sent from Deep Discovery Inspector is blocked by our security product as a phishing URL?

This may be due to your network’s security policies. Add Deep Discovery Inspector to your network security product’s white list.

After a fresh installation, Deep Discovery Inspector is unable to obtain a dynamic IP address. What do I do?

Restart the appliance and verify that it is able to obtain an IP address. Next, connect an ethernet cable from the management port to a known good ethernet connection and restart the appliance.
If I navigate away from the Appliance IP Settings page or log off the web console after capturing network packets, my network packet capture are lost. How do I avoid this?

Be sure to export the network packet capture result to your local hard drive before navigating away from the Appliance IP Settings page or logging off of Deep Discovery Inspector.

**Detections**

Why does no data appear on the Detections page after I activate Deep Discovery Inspector but it does appear if I do a Detections Log Query?

It takes up to 10 minutes to aggregate Detections data.

**Widgets**

Why are widget heights inconsistent, even though Auto-fit is enabled in the Tab Settings?

The Auto-fit function depends on the layout option selected and how many widgets are added. Auto-fit is enabled only when the selected widgets can be arranged one widget per field.

**Logs**

I tried to export the logs from the web console, but was unable to select a file extension. What should I do?

If you are using IE9 as your browser, this happens when the Do not save encrypted pages to disk option is enabled. To change this, in an IE9 browser window go to Tools > Internet Options > Advanced tab > Security section > uncheck Do not save encrypted pages to disk, and click OK to apply changes. Open a new browser window and re-export the logs.

How can I cancel the export window while exporting Deep Discovery Inspector logs using IE9?

Open IE9 and go to Tools > Internet Options > Advanced tab > Security section > uncheck Do not save encrypted pages to disk. Click OK to apply changes. Open a new browser window and export logs.
Why does the Log Query screen display no result or takes a long time before the results appear?

When Deep Discovery Inspector queries the database, you may experience some slight delay before the query results appear, especially if there is heavy network traffic. Please wait for the query results to be displayed. If you click Search again before the query results appear Deep Discovery Inspector re-queries the logs.

Virtual Analyzer

I imported the virtual analyzer image into Deep Discovery Inspector. When I tried to import the same image again, it failed. What can I do?

This happens because Deep Discovery Inspector records each image’s unique identification. An image with the same unique identification cannot be imported twice consecutively if the first import was successful, due to a known VirtualBox issue. Create a new image and go to Appendix A to re-import a new image.

Troubleshooting

During Deep Discovery Inspector rescue operation I get an error message with random text. Now what?

Remove any USB storage devices connected to Deep Discovery Inspector and try again.

Product Updates

By default, where does Deep Discovery Inspector download updated components from?

Deep Discovery Inspector 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 Deep Discovery Inspector?

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

Does Deep Discovery Inspector restart during an update?

Yes, Deep Discovery Inspector will restart after Network Content Inspection Engine and Deep Discovery Inspector firmware updates. For scheduled updates, Deep Discovery Inspector sends an email to the user to click the Restart button in the product console. For manual updates, the Restart button appears in the Manual Update screen until you restart the product.

Why does Deep Discovery Inspector still use the old components after updating the software and restarting the product?

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

Documentation

What documentation is available with this version of Deep Discovery Inspector?

This version of Deep Discovery Inspector includes the following documentation:

• Administrator's Guide
• Readme file
• Help

Upgrading from Threat Discovery Appliance 2.6 or Deep Discovery 3.0

Can I upgrade Threat Discovery Appliance 2.6 or Deep Discovery 3.0 to Deep Discovery Inspector 3.2?

No. You will need to obtain a new license for Deep Discovery Inspector and do a fresh installation.
Before Contacting Technical Support

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

Trend Community
Get help, share your experiences, ask questions, and discuss security concerns with other fellow users, enthusiasts, and security experts.

http://community.trendmicro.com/

The Trend Micro Support Portal
The Trend Micro Support Portal has the most up-to-date answers to product questions. Use the Support Portal to submit a query for issues not found in the product documentation. Access the Support Portal at:

http://esupport.trendmicro.com

Trend Micro updates the contents of the Support Portal continuously and adds new solutions daily. For issues not found within the Portal, describe the problem in an email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

Security Information Center
Comprehensive security information is available at the Trend Micro website.

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

Security information includes:
• List of viruses and malicious mobile code currently "in the wild," or active
• Computer virus hoaxes
• Internet threat advisories
• Virus weekly report
• Virus Encyclopedia
• Glossary of terms
Contacting Trend Micro

Technical Support

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

Trend Micro Incorporated provides worldwide support to all registered users.

Get a list of the worldwide support offices at:

http://www.trendmicro.com/support

Get the latest Trend Micro product documentation at:

http://downloadcenter.trendmicro.com/

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

Trend Micro, Inc.
10101 North De Anza Blvd., Cupertino, CA 95014
Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address:

http://www.trendmicro.com
Email: support@trendmicro.com
Getting Help

Calling Support
To speed up problem resolution when calling Trend Micro support, ensure that the following details are available:

• Microsoft Windows and Service Pack versions
• Network type
• Computer brand, model, and any additional hardware connected to your workstation
• Amount of memory and free hard disk space on your workstation
• Detailed description of the installation environment
• Exact text of any error message given
• What steps to take to reproduce the problem

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

You can rely on the following post-sales service:

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

TrendLabs has achieved ISO 9002 quality assurance certification.

Sending Suspicious Files to Trend Micro
If you think you have an infected file but the scan engine does not detect it or cannot clean it, Trend Micro encourages you to send the suspect file to us.
You can also send Trend Micro the URL of any website you suspect of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and viruses).

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

virusresponse@trendmicro.com

You can also use the web submission form at:


**Documentation Feedback**

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

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

This glossary describes terms related to Deep Discovery Inspector use.

**TABLE 10-1. Glossary of Terms**

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>This refers to the device currently in use.</td>
</tr>
<tr>
<td>ActiveUpdate</td>
<td>ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update website, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, program, and other Trend Micro component files through the Internet or the Trend Micro Total Solution CD.</td>
</tr>
<tr>
<td>ActiveX</td>
<td>A type of open software architecture that implements object linking and embedding, enabling standard interfaces (downloading of web pages).</td>
</tr>
<tr>
<td>ActiveX control</td>
<td>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.</td>
</tr>
</tbody>
</table>
Hackers and virus writers use ActiveX malicious code as a vehicle to attack the system. Changing your browser's security settings to "high" is a proactive approach to keep ActiveX controls from executing.

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 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.

Advanced Threat Scan Engine
Checks files for less conventional threats, including document exploits. Some detected files may be safe and should be further observed and analyzed in a virtual environment.

Adware
Advertising-supported software that allows advertising banners to appear while the program is running. See also Spyware.

Alert
A message intended to inform a system's users or administrator about a change in the system's operating conditions or about some kind of error condition.

Antivirus
Computer programs designed to detect and clean computer viruses.
### Glossary of Terms (Continued)

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>APT</td>
<td>Advanced Persistent Threats (APTs) are targeted attacks with a pre-determined objective: steal sensitive data or cause targeted damage. The objective is not the defining attribute of this type of attack; it’s the fact that attackers are persistent in achieving their objective.</td>
</tr>
<tr>
<td>Archive</td>
<td>A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program (a .zip file).</td>
</tr>
<tr>
<td>ATSE</td>
<td>See also Advanced Threat Scan Engine.</td>
</tr>
<tr>
<td>Attachment</td>
<td>A file attached to (sent with) an email message.</td>
</tr>
</tbody>
</table>
| 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 designated portion of a disk (the physical device from which the computer reads and writes data). The boot sector contains the data used by your computer to load and initialize the computer’s operating system. |
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 an external drive - the boot attempt does not have to be successful for the virus to infect the hard drive.

Once the system is infected, the boot sector virus attempts to infect every disk accessed by that computer. Most antivirus software can successfully remove boot sector viruses.

Botnet | see Command and Control (C&C) server

Bridge | A device that forwards traffic between network segments based on data link layer (.dll) information. These segments have a common network layer address.

Browser | A program (Internet Explorer, Chrome, Firefox) that enables the reading of hypertext. The browser allows the viewing of node contents (pages) and navigation from one node to another. A browser acts as a host 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.

Command and Control (C&C) server | The central server(s) for a botnet or entire network of compromised devices used by a malicious bot to propagate malware and infect a host.
<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communicator</td>
<td>The communications backbone of the Control Manager system; it is part of the Trend Micro Management Infrastructure. Commands from the Control Manager server to Deep Discovery Inspector, and status reports from Deep Discovery Inspector to the Control Manager server all pass through this component.</td>
</tr>
<tr>
<td>Compressed file</td>
<td>A single file containing one or more separate files plus information for extraction by a suitable program, (WinZip).</td>
</tr>
<tr>
<td>Configuration</td>
<td>The process of selecting options for how Deep Discovery Inspector (and other Trend Micro products) function.</td>
</tr>
<tr>
<td>Control Manager Server</td>
<td>The server associated with Trend Micro Control Manager, upon which TMCM is installed. This server hosts the web-based TMCM product console.</td>
</tr>
<tr>
<td>Cookie</td>
<td>A mechanism for storing information about an Internet user (name, preferences, and interests) in your web browser for later use. The next time you access a website for which your browser has a cookie, your browser sends the cookie to the web server, which the web server can then use to present you with customized web pages. Example: entering a website that welcomes you by name.</td>
</tr>
<tr>
<td>Daemon</td>
<td>A program not explicitly invoked that lays dormant waiting for some condition(s) to occur. User are typically not aware that a daemon is lurking and my inadvertently cause the condition to occur which invokes the daemon.</td>
</tr>
</tbody>
</table>
### TABLE 10-1. Glossary of Terms (Continued)

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>A preset value that populates a field in the management console interface. A default value typically represents a logical (recommended) choice and is provided for convenience. Some default values are static, others can be changed.</td>
</tr>
<tr>
<td>Denial of Service (DoS) attack</td>
<td>Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.</td>
</tr>
<tr>
<td>Virtual Analyzer</td>
<td>Deep Discovery Inspector’s threat analysis tool in the form of either a built-in virtual analyzer or Deep Discovery Advisor.</td>
</tr>
<tr>
<td>Detections</td>
<td>Signature-based detection involves searching for known patterns of data within executable code.</td>
</tr>
<tr>
<td>Dialer</td>
<td>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 their knowledge.</td>
</tr>
<tr>
<td>Digital signature</td>
<td>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.</td>
</tr>
<tr>
<td>Directory</td>
<td>Part of the structure (node) on a hierarchical computer file system. A directory typically contains other nodes, folders, or files. Example: C:\Windows is the Windows directory on the C drive.</td>
</tr>
<tr>
<td>Directory path</td>
<td>The subsequent layers within a directory where a file can be found. Example: the directory path for the ISVW for SMB Quarantine directory is: C:\Programs\Trend Micro\ISVW\Quarantine</td>
</tr>
</tbody>
</table>
### Glossary of Terms (Continued)

<table>
<thead>
<tr>
<th><strong>TERM</strong></th>
<th><strong>DEFINITION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclaimer</td>
<td>A statement appended to the beginning or end of an email message that states certain terms of legality and confidentiality regarding the message.</td>
</tr>
<tr>
<td>Disruptive Applications</td>
<td>Instant messaging, streaming media, and peer-to-peer applications are considered to be disruptive because they slow down the network, are a security risk, and can be a distraction to employees.</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System—A general-purpose data query service used for translating Internet host names into IP addresses.</td>
</tr>
<tr>
<td>DNS resolution</td>
<td>When a DNS host requests host name and address data from a DNS server, the process is called <em>resolution</em>.</td>
</tr>
<tr>
<td></td>
<td>Basic DNS configuration results in a server that performs default resolution. Example: a remote server queries another server for computer data in the current zone. Client software in the remote server queries the resolver, which answers the request from its database files.</td>
</tr>
<tr>
<td>(Administrative) domain</td>
<td>A group of computers sharing a common database and security policy.</td>
</tr>
<tr>
<td>Domain name</td>
<td>The full name of a system, consisting of its local host name and its domain name. Example: tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host in the Internet. This process, called &quot;name resolution&quot;, uses the Domain Name System (DNS).</td>
</tr>
</tbody>
</table>
TABLE 10-1. Glossary of Terms (Continued)

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOS virus</td>
<td>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 replicate and spread by infecting other host programs.</td>
</tr>
<tr>
<td>Download</td>
<td>The process of transferring data or code from one computer to another. Downloading often refers to a transfer from a larger &quot;host&quot; system (especially a server or mainframe) to a smaller &quot;host&quot; system.</td>
</tr>
<tr>
<td>Dropper</td>
<td>Droppers are programs that serve as delivery mechanisms to carry and drop viruses, Trojans, or worms into a system.</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol (DHCP)</td>
<td>A protocol for assigning dynamic IP addresses to devices in a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. DHCP also supports a mixture of static and dynamic IP addresses.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Encryption is the form of data protection that changed data into a form that only the intended receiver can read.</td>
</tr>
<tr>
<td>Entity</td>
<td>A representation of a managed product (Deep Discovery Inspector) on the TMCM console’s directory tree, including all managed entities.</td>
</tr>
<tr>
<td>Ethernet</td>
<td>A local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. which can be used to connect to the internet</td>
</tr>
<tr>
<td>Executable file</td>
<td>A binary file containing a program in computer language which is ready to be executed (run).</td>
</tr>
<tr>
<td>TERM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EXE file infector</td>
<td>An executable program with an .exe file extension. <em>Also see DOS virus.</em></td>
</tr>
<tr>
<td>Exploit</td>
<td>Network and file-based exploit attempts</td>
</tr>
<tr>
<td>False positive</td>
<td>An email message that was &quot;caught&quot; by the spam filter and identified as spam, but is actually not spam.</td>
</tr>
<tr>
<td>FAQ</td>
<td>Frequently Asked Questions—A list of questions and answers about a specific topic.</td>
</tr>
<tr>
<td>File</td>
<td>An discrete data element.</td>
</tr>
<tr>
<td>File-infecting virus</td>
<td>File-infecting viruses infect executable programs (files with .com or .exe extensions). Most file-infecting viruses replicate and spread by infecting other host programs.\nIn 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 is unrecoverable</td>
</tr>
<tr>
<td>File type</td>
<td>Any data stored in a file. Most operating systems use the file name extension to determine 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.</td>
</tr>
<tr>
<td>File name extension</td>
<td>The portion of a file name (.dll or .xml) which indicates the application used to create the file.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Security settings used to control traffic to/from endpoints.</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol - a client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network.</td>
</tr>
<tr>
<td>TERM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Gateway</td>
<td>An interface between an information source and a web server.</td>
</tr>
<tr>
<td>Grayware</td>
<td>A category of software that may be legitimate, unwanted, or malicious. Unlike viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data. Example: spyware, adware, and remote access tools.</td>
</tr>
<tr>
<td>GRID</td>
<td>GRID (Goodware Resource and Information Database) is a Trend Micro list of known good files, codes, and URLs. It is used to differentiate files that are safe from those that aren’t. Enabling this option allows selected files to be scanned and classified prior to being submitted to the Virtual Analyzer.</td>
</tr>
<tr>
<td>Hacker</td>
<td>See virus writer.</td>
</tr>
<tr>
<td>Hard disk (hard drive)</td>
<td>One or more rigid magnetic disks rotating about a central axle used to read and write hard disks and to store data. Hard disks can be permanently connected to the drive (fixed disks) or external to an endpoint.</td>
</tr>
<tr>
<td>Heuristic rule-based scanning</td>
<td>Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.</td>
</tr>
<tr>
<td>Host</td>
<td>Any device attached to a network.</td>
</tr>
<tr>
<td>HTML virus</td>
<td>A virus targeted at Hyper Text Markup Language (HTML), the authoring language used to create information on a web page. The virus resides on a web page and downloads through a user’s browser.</td>
</tr>
<tr>
<td>HTTP</td>
<td>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.</td>
</tr>
</tbody>
</table>

TABLE 10-1.  Glossary of Terms (Continued)
<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure—A type of HTTP for handling secure transactions.</td>
</tr>
<tr>
<td>iDRAC</td>
<td>In computing, the Dell Remote Access Controller or DRAC, an interface card from Dell Inc, provides out-of-band management facilities. The controller has its own processor, memory, network connection, and access to the system bus. Key features include power management, virtual media access and remote console capabilities, all available through a supported web browser or command line interface. This gives system administrators the ability to configure a machine as if they were sitting at the local console (terminal).</td>
</tr>
<tr>
<td>Image</td>
<td>Refers to Trend Micro Deep Discovery Inspector firmware or program file that can be configured, imported, and exported.</td>
</tr>
<tr>
<td>IntelliScan</td>
<td>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 harbor malicious code. True file type recognition helps identify malicious code hiding behind a known safe extension name.</td>
</tr>
<tr>
<td>IntelliTrap</td>
<td>IntelliTrap helps reduce the risk of such viruses entering the network by blocking real-time compressed executable files and pairing them with other malware characteristics.</td>
</tr>
</tbody>
</table>
Internet Safety Tips

Most malware threats are introduced onto endpoints through attack vectors and protocols. One tactic is to use social engineering to entice, intimidate, or trick the "victim" into clicking a URL that runs malicious code. Malicious code can also arrive as an email attachment, a file transfer request in an IM application, transparently installed with other "free" software, or disguised as "safe" software, document, or media. Clicking a malicious URL link can open the user's browser to a web page that installs the malware, if the browser is vulnerable. Malware disguised as software the "victim" is interested in (a "necessary" update needed to view an online video, a serial key generator, or "free" cracked copy of some popular software). Automatic propagation through open, vulnerable services or network shares makes it critically important to enforce strong passwords and to maintain hosts on a network with up-to-date OS, browser, and application patches.

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Safety Tips</td>
<td>Most malware threats are introduced onto endpoints through attack vectors and protocols. One tactic is to use social engineering to entice, intimidate, or trick the &quot;victim&quot; into clicking a URL that runs malicious code. Malicious code can also arrive as an email attachment, a file transfer request in an IM application, transparently installed with other &quot;free&quot; software, or disguised as &quot;safe&quot; software, document, or media. Clicking a malicious URL link can open the user's browser to a web page that installs the malware, if the browser is vulnerable. Malware disguised as software the &quot;victim&quot; is interested in (a &quot;necessary&quot; update needed to view an online video, a serial key generator, or &quot;free&quot; cracked copy of some popular software). Automatic propagation through open, vulnerable services or network shares makes it critically important to enforce strong passwords and to maintain hosts on a network with up-to-date OS, browser, and application patches.</td>
</tr>
<tr>
<td>IP address</td>
<td>Internet address for a device in a network, typically expressed using dot notation: 123.123.123.123.</td>
</tr>
<tr>
<td>IP gateway</td>
<td>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.</td>
</tr>
<tr>
<td>IT</td>
<td>The field of Information Technology which includes hardware, software, networking, telecommunications, and user support.</td>
</tr>
<tr>
<td>Java file</td>
<td>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.</td>
</tr>
<tr>
<td>TERM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Java malicious code</td>
<td>Virus code written or embedded in Java. Also see Java file.</td>
</tr>
<tr>
<td>JavaScript</td>
<td>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.</td>
</tr>
<tr>
<td>JavaScript virus</td>
<td>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.</td>
</tr>
<tr>
<td>Known Malware</td>
<td>Files known to contain malware</td>
</tr>
<tr>
<td>Keylogger</td>
<td>Keyloggers are programs that catch and store all keyboard activity.</td>
</tr>
<tr>
<td>L2 devices</td>
<td>Short for layer 2 devices. These are hardware devices (switches) connected to the Data Link Layer of the OSI model.</td>
</tr>
<tr>
<td>L3 devices</td>
<td>Short for layer 3 devices. These devices refer to the hardware devices (routers) connected to the Network layer of the OSI model.</td>
</tr>
<tr>
<td>Link (hyperlink)</td>
<td>A reference from some point in one hypertext document to some point in another document or another place in the same document.</td>
</tr>
<tr>
<td>Listening port</td>
<td>A port utilized for host connection requests for data exchange.</td>
</tr>
<tr>
<td>Logs</td>
<td>A time-based collection of data history which can be saved, imported, or exported as a discrete file.</td>
</tr>
<tr>
<td>Macro</td>
<td>A command used to automate certain application functions.</td>
</tr>
</tbody>
</table>
MacroTrap | A Trend Micro utility that performs a rule-based examination of all macro code saved with a document.

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.

Macro virus code | Macro virus code is contained in part of the template that travels with many documents (.dot in Microsoft Word documents).

Malicious Behavior | Positively-identified malware communications, known malicious destination contacted, malicious behavioral patterns and strings that definitely indicate compromise with no further correlation needed.

Malicious URL | See Web Reputation.

Malware (malicious software) | Programming or files developed for the purpose of doing harm, such as viruses, worms, and Trojans.

Management Communication Protocol (MCP) Agent | An application installed along with Deep Discovery Inspector that allows Control Manager to manage the product. The agent receives commands from the Control Manager server, and then applies them to Deep Discovery Inspector. It also collects logs from the product, and sends them to Control Manager. The Control Manager agent does not communicate with the Control Manager server directly. Instead, it interfaces with a component called the Communicator.

Management (web) console | The user interface for your Trend Micro product.
<table>
<thead>
<tr>
<th><strong>TERM</strong></th>
<th><strong>DEFINITION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mass mailer (Worm)</td>
<td>A malicious program that has high damage potential, due to the large amounts of network traffic it generates.</td>
</tr>
<tr>
<td>Mbps</td>
<td>Millions of bits per second—a measure of bandwidth in data communications.</td>
</tr>
<tr>
<td>MCP Agent</td>
<td>Management Communication Protocol Agent - used to communicate with TMCM.</td>
</tr>
<tr>
<td>Message</td>
<td>An email message, which includes the message subject in the message header and the message body.</td>
</tr>
<tr>
<td>Message body</td>
<td>The content of an email message.</td>
</tr>
<tr>
<td>Message size</td>
<td>The number of KB or MB occupied by a message and its attachments.</td>
</tr>
<tr>
<td>Message subject</td>
<td>The title or topic of an email message, such as “Third Quarter Results” or “Lunch on Friday.”</td>
</tr>
<tr>
<td>Microsoft Office file</td>
<td>Files created with Microsoft Office.</td>
</tr>
<tr>
<td>Mirror port</td>
<td>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.</td>
</tr>
<tr>
<td>Mixed threat attack</td>
<td>Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks.</td>
</tr>
<tr>
<td>Multi-partite virus</td>
<td>A virus that has characteristics of both boot sector viruses and file-infecting viruses.</td>
</tr>
</tbody>
</table>
### TABLE 10-1. Glossary of Terms  (Continued)

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address Translation (NAT)</td>
<td>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.</td>
</tr>
<tr>
<td>NetBIOS (Network Basic Input Output System)</td>
<td>An application program interface (API) that adds functionality (network capabilities) to disk operating system (DOS) basic input/output system (BIOS).</td>
</tr>
<tr>
<td>Network segment</td>
<td>A section of a network that falls within the bounds of bridges, routers, or switches.</td>
</tr>
<tr>
<td>Network tap</td>
<td>A test access point or hardware device which provides a way to access the data flowing across a computer network. In many cases, it is desirable for a third party to monitor the traffic between two points in the network.</td>
</tr>
<tr>
<td>Network Time Protocol (NTP)</td>
<td>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.</td>
</tr>
<tr>
<td>Network virus</td>
<td>A type of virus that uses network (TCP, FTP, UDP, HTTP) and email protocols to replicate.</td>
</tr>
<tr>
<td>Notification</td>
<td>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 to communicate that an action took place, or been attempted. Also see action and target.</td>
</tr>
</tbody>
</table>
TABLE 10-1. Glossary of Terms (Continued)

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offensive content</td>
<td>Words or phrases in messages or attachments that are considered offensive to others: profanity, sexual harassment, racial harassment, or hate mail.</td>
</tr>
<tr>
<td>Open source</td>
<td>Programming code available to the general public for use or modification free-of-charge and without license restrictions.</td>
</tr>
<tr>
<td>Operating System (OS)</td>
<td>Software that handles tasks including the interface to peripheral hardware, scheduling tasks, and allocating storage.</td>
</tr>
<tr>
<td>Open System Interconnection (OSI) model</td>
<td>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, proceeding to the bottom layer, over the channel and back up the hierarchy.</td>
</tr>
<tr>
<td>Outbreak Containment Service (OCS)</td>
<td>Detects both known and unknown malware that can potentially start an outbreak.</td>
</tr>
<tr>
<td>Outgoing</td>
<td>Email messages or other data leaving your network.</td>
</tr>
<tr>
<td>Packer</td>
<td>A compression tool for executable files.</td>
</tr>
<tr>
<td>Partition</td>
<td>A logical portion of a disk.</td>
</tr>
<tr>
<td>Password cracker</td>
<td>An application program used to recover a lost or forgotten password. These can be used to gain unauthorized access to an endpoint.</td>
</tr>
<tr>
<td>Pattern file (Official Pattern Release)</td>
<td>The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses.</td>
</tr>
<tr>
<td>Payload</td>
<td>Payload refers to an action that a virus performs on an infected endpoint: displaying messages or ejecting the CD drive (harmless) or deleting the entire hard drive (harmful).</td>
</tr>
<tr>
<td>TERM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Polymorphic virus</td>
<td>A virus capable of taking different forms.</td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol, version 3—A messaging protocol that allows a host computer to retrieve electronic mail from a server through a temporary connection.</td>
</tr>
<tr>
<td>POP3 server</td>
<td>A server which hosts POP3 email, from which clients on your network retrieve POP3 messages.</td>
</tr>
<tr>
<td>Port</td>
<td>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.</td>
</tr>
<tr>
<td>Port mirroring</td>
<td>Method of monitoring network traffic by copying source port or VLAN specific traffic to a destination port for analysis.</td>
</tr>
<tr>
<td>Pre-configuration</td>
<td>The console used to preconfigure the device.</td>
</tr>
<tr>
<td>Console</td>
<td></td>
</tr>
<tr>
<td>Proxy</td>
<td>A process of providing a cache of items available on other servers, which are presumably slower or more expensive to access.</td>
</tr>
<tr>
<td>Proxy server</td>
<td>A server which accepts URLs with a special prefix, used to access documents from either a local cache or a remote server, then returns the URL to the requester.</td>
</tr>
<tr>
<td>Purge</td>
<td>To delete all, as in getting rid of old entries in the logs.</td>
</tr>
<tr>
<td>Recipient</td>
<td>The person or entity to whom an email message is addressed.</td>
</tr>
<tr>
<td>TERM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registered Domain</td>
<td>A domain used for internal purposes or those considered trustworthy, to establish the network profile.</td>
</tr>
<tr>
<td>Registered Service</td>
<td>A server for specific services that is used internally or is considered trustworthy, to establish the network profile.</td>
</tr>
<tr>
<td>Reports</td>
<td>A compilation of data generated from selectable criteria, used to provide the user with needed information.</td>
</tr>
<tr>
<td>Remote Port Mirroring</td>
<td>An implementation of port mirroring designed to support source ports, source VLANs, and destination ports across different switches.</td>
</tr>
<tr>
<td>Removable drive</td>
<td>A removable hardware component or peripheral device of an endpoint.</td>
</tr>
<tr>
<td>RJ-45</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual Analyzer</td>
<td>An environment on a network, where suspect files can be isolated in order to observe and analyze their behavior.</td>
</tr>
<tr>
<td>Scan</td>
<td>To examine items in a file in sequence to find those that meet a particular criteria.</td>
</tr>
<tr>
<td>Scan engine</td>
<td>The module that performs antivirus scanning and detection in the host product to which it is integrated.</td>
</tr>
<tr>
<td>Secure Password Authentication</td>
<td>An authentication process, designed to protect digital communication.</td>
</tr>
</tbody>
</table>
Secure Socket Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols.

The person who sends an email message to another person or entity.

A program that provides a service to other (host) program(s) using a network connection and various protocol to encode the host's requests and the server's responses.

Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers. It is a server-to-server protocol but uses other protocols to access messages.

A server that relays email messages to their destinations.

Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for possible administrative attention.

A software module, in a managed device, which communicates with the network management server.

A programming mechanism that handles errors or other problems on a computer program related to network device monitoring.

A protocol that relays transmission control protocol (TCP) sessions at a firewall host to allow application users transparent access across the firewall.

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Socket Layer (SSL)</td>
<td>Secure Socket Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols.</td>
</tr>
<tr>
<td>Sender</td>
<td>The person who sends an email message to another person or entity.</td>
</tr>
<tr>
<td>Server</td>
<td>A program that provides a service to other (host) program(s) using a network connection and various protocol to encode the host's requests and the server's responses.</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers. It is a server-to-server protocol but uses other protocols to access messages.</td>
</tr>
<tr>
<td>SMTP server</td>
<td>A server that relays email messages to their destinations.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for possible administrative attention.</td>
</tr>
<tr>
<td>SNMP agent</td>
<td>A software module, in a managed device, which communicates with the network management server.</td>
</tr>
<tr>
<td>SNMP trap</td>
<td>A programming mechanism that handles errors or other problems on a computer program related to network device monitoring.</td>
</tr>
<tr>
<td>SOCKS4</td>
<td>A protocol that relays transmission control protocol (TCP) sessions at a firewall host to allow application users transparent access across the firewall.</td>
</tr>
<tr>
<td>Spam</td>
<td>Unsolicited email messages</td>
</tr>
</tbody>
</table>
### TABLE 10-1. Glossary of Terms (Continued)

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware</td>
<td>Advertising-supported software that installs tracking software in your system, capable of sending information about you to another party.</td>
</tr>
<tr>
<td>Strong Password</td>
<td>A password that contains upper case letters, lower case letters, plus punctuation and symbols.</td>
</tr>
<tr>
<td>Suspicious Behavior</td>
<td>Anomalous behavior, false or misleading data, suspicious and malicious behavioral patterns and strings that could indicate system compromise but needs further correlation to confirm.</td>
</tr>
<tr>
<td>Switch</td>
<td>A networked device that filters and forwards packets between LAN segments.</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol - the basic communication language (protocol) of the Internet.</td>
</tr>
<tr>
<td>Threat Connect</td>
<td>A Trend Micro service used to provide details about detected threat behavior.</td>
</tr>
<tr>
<td>Traffic</td>
<td>Data flowing between the Internet and your network, both incoming and outgoing.</td>
</tr>
<tr>
<td>Traffic Mirroring</td>
<td>Used on network appliances that require monitoring of network traffic, 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.</td>
</tr>
<tr>
<td>Trend Micro Control Manager</td>
<td>An intuitive web console for centralized management of Trend Micro products and services.</td>
</tr>
<tr>
<td>Trojan Horse</td>
<td>A malicious executable program disguised as something benign that resides in a system and is used to perform malicious acts.</td>
</tr>
<tr>
<td>TERM</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>True file type</td>
<td>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.</td>
</tr>
<tr>
<td>Trusted domain</td>
<td>A domain from which your Trend Micro product always accepts messages, without considering whether the message is spam.</td>
</tr>
<tr>
<td>Trusted host</td>
<td>A server allowed to relay mail through your network because they are trusted to act appropriately.</td>
</tr>
<tr>
<td>URL</td>
<td>Universal Resource Locator—A standard method of specifying the location of an object on the Internet.</td>
</tr>
<tr>
<td>Virtual Analyzer</td>
<td>A Trend Micro product designed to isolate suspect files in order to observe and analyze their behavior.</td>
</tr>
<tr>
<td>Virtual SMP</td>
<td>Virtual Symmetric Multi-processor - a VMWare feature that enables assigning of multiple, physical CPUs to a virtual machine.</td>
</tr>
<tr>
<td>VBscript</td>
<td>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.</td>
</tr>
<tr>
<td>VBscript virus</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual Local Area Network (VLAN)</td>
<td>A logical (not physical) grouping of devices that constitutes a single broadcast domain. See the IEEE 802.1Q standard for additional details.</td>
</tr>
</tbody>
</table>
### Glossary

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.

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus kit</td>
<td>A template of source code for building and executing a virus.</td>
</tr>
<tr>
<td>Virus signature</td>
<td>A unique string of bits that identifies a specific virus, stored in the Trend Micro virus pattern file for comparison to known viruses. If the scan engine detects a match it cleans, deletes, and/or quarantines the virus, according to your security policy.</td>
</tr>
<tr>
<td>Virus writer</td>
<td>A computer hacker, someone who writes virus code.</td>
</tr>
<tr>
<td>Web</td>
<td>The World Wide Web, also called the web or the Internet.</td>
</tr>
<tr>
<td>Web Reputation</td>
<td>Any website (URL) that tries to perform malicious activities: Trojan Horse programs, spyware, adware, Pharming and other malware.</td>
</tr>
<tr>
<td>Widget</td>
<td>A customizable screens used to view specific, selected data sets.</td>
</tr>
<tr>
<td>Widget Framework</td>
<td>The template for creating widget structure.</td>
</tr>
<tr>
<td>Wildcard</td>
<td>A term used in reference to content filtering, where an asterisk (*) represents any characters.</td>
</tr>
<tr>
<td>Worm</td>
<td>A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.</td>
</tr>
<tr>
<td>Zip file</td>
<td>A compressed archive (.zip file) from one or more files using an archiving program such as WinZip.</td>
</tr>
</tbody>
</table>
Creating a Custom Virtual Analyzer

Creating a Custom Virtual Analyzer

This chapter explains how to:

- convert a VMware image into a custom virtual analyzer image
- use VirtualBox to create a custom virtual analyzer image.

Administrators can use a custom virtual analyzer as an isolated environment, external from the corporate network, to monitor and analyze suspicious files and file behaviors, in order to determine whether a file is malicious. Deep Discovery Inspector-related custom virtual analyzers are designed to provide a secure environment and, since they can be isolated from the corporate network, do not impact network performance.

The topics discussed in this appendix are:

- *Converting VMware Image with VMware Converter* on page A-3
- *Creating a Virtual Analyzer Image with VirtualBox* on page A-11
- *Using VirtualBox to Export an OVA Image* on page A-33
- *Uploading Virtual Machine Images to Deep Discovery Inspector and Configuring Virtual Analyzer* on page A-43
- *Troubleshooting* on page A-45
Converting a VMware Image

This section explains how to:

- prepare the VMware Workstation, VMPlayer, or ESXi server image to be used by VirtualBox
- install applications
- configure an automatic login
- convert an image with VirtualBox.

Install the VMware Converter Tool:

http://downloads.vmware.com/d/info/infrastructure_operations_management/vmware_vcenter_converter_standalone/5.0

Note: Uninstall the VMware Converter Tool before creating the image.

Installing Applications

Verify that all needed applications have been configured on the virtual machine prior to converting a VMware image. See Installing Applications on page A-31.

Configuring Automatic Login

Verify that auto login has been configured on the virtual machine prior to converting a VMware image. See Configuring Automatic Login on page A-32.
Creating a Custom Virtual Analyzer

Converting VMware Image with VMware Converter

1. Open VMware vCenter Converter Standalone and select **Connect to a local server.**

   ![VMware Login Window](image)

   **FIGURE A-1. VMware Login Window**

2. Click **Login.**

   The Welcome to VMware vCenter Converter Standalone window appears.
3. Click **Convert Machine**.
   The Conversion Source System window appears.

4. At the Conversion Source System window, use the following settings:
   - **Select source type**: VMware Workstation or other VMware virtual machine
   - **Virtual machine file**: Click Browse to choose the VMX file of the image to be converted.
5. Click **Next**.
   The Conversion Source Destination window appears.

6. At the Conversion Source Destination window, use the following settings:
   - **Select destination type**: VMware Workstation or other VMware virtual machine
   - **Select VMware product**: VMware Workstation 6.5.x
   - **Virtual machine details**:
     - **Name**: Use default or type a name.
     - **Select a location for the virtual machine**: Type a destination.

7. Click **Next**.
   The Conversion Options window appears. See Figure A-4 for options.

8. Click **Edit** to update options.
9. Click **Edit** for **Data to copy** to verify that the type for VirtualDisk1 is set to *Not pre-allocated*.
10. Click **Edit** for Advanced options.
    
The Pre-conversion menu appears.

11. At the Pre-conversion menu unmark **Install VMware Tools on the destination virtual machine.**
12. Click **Next**.
   The Summary screen appears.

13. Verify the information that appears on the Summary screen.

**FIGURE A-6. Unmark Install VMware Tools Window**

15. When the process is complete, record the converted image (VMDK) path.
**FIGURE A-8.** Conversion Window
Creating a Virtual Analyzer Image with
VirtualBox

Deep Discovery Inspector's virtual machine tool is VirtualBox. Use the following
method to create a virtual Virtual Analyzer image.

Downloading and Installing VirtualBox

![VirtualBox Logo](image)

**FIGURE A-9. VirtualBox Logo**

1. Download the latest version of VirtualBox:
   
   [https://www.virtualbox.org/wiki/Downloads](https://www.virtualbox.org/wiki/Downloads)

2. Install VirtualBox on your local machine using an English language default.
   
   a. If needed, configure language settings after installation:
      
      File > Preferences > Language > English.
Preparing the Operating System ISO

Note: The Deep Discovery Inspector Virtual Analyzer currently only supports English versions of Windows XP and Windows 7.
Create a new Virtual Analyzer Image

1. Click on the **New** icon at the top-left of the VirtualBox Manager window.
2. At the Create New Virtual Machines window, click Next.
The VM Name and OS Type window appears.

![Figure A-13. VM Name and OS Type Window](image.png)

3. Type the name of the virtual machine, its operating system, and version and click Next.
The Memory window appears.
4. At the Memory window, use the slider to select the base memory size and click Next.
   Select 512 MB for Windows XP.
   Select 1024 MB for Windows 7.
   The Virtual Hard Disk window appears.
FIGURE A-15. Virtual Hard Disk Window

5. At the Virtual Hard Disk window select **Create new hard disk** and click **Next**. The Virtual Disk Creation Wizard window appears.

FIGURE A-16. Virtual Disk Creation Wizard Window
6. At Virtual Disk Creation Wizard window, select **VMDK (Virtual Machine Disk)** and click **Next**.
   The Virtual disk storage details window appears.

   ![Virtual Disk Store Details Window](image)

   **FIGURE A-17. Virtual Disk Store Details Window**

7. At Virtual disk storage details window > Storage details, select **Dynamically allocated** and click **Next**.
   The Virtual disk file location and size window appears.
8. Click the folder icon to change the path of the virtual disk file, if needed.

9. Use the slider to select the virtual disk size and click Next.
   For Windows XP, set the image size to 15 GB.
   For Windows 7, set the image size to 25 GB.

   FIGURE A-18. Virtual Disk File Location and Size Window

   The Summary window appears.
10. Review these settings and click **Create**.

The VirtualBox Manager lists all virtual machines available for use; any virtual machines that were created are listed on the left pane.

11. On the VirtualBox Manager window, click the **Settings** icon.
The VirtualBox setting options are displayed.

**FIGURE A-21. VirtualBox Setting Options**

12. On the Settings options window, click **System**. The System options are displayed.

**FIGURE A-22. Virtual Analyzer System Options**
13. At the Systems options, select the Motherboard tab and set the following:
   - Chipset to ICH9
   - Check Enable IO APIC
   - Uncheck Enable absolute pointing device
14. At the Systems options, select the Processor tab and set the following:
   - Check Enable PAE/NX.
15. On the Settings options window, click Storage.
    The Storage options are displayed.

![Virtual Analyzer Storage Settings Window](image)

**FIGURE A-23.** Virtual Analyzer Storage Settings Window

16. At the Storage options window, set the following
    - Storage Tree to Empty.
17. Under Attributes, click the CD icon (to the right of CD/DVD Drive).
    A file menu appears.
18. Select Choose a virtual CD/DVD disk file… and the OS ISO to install.
    The disk file is available as a device.
    The Audio options are displayed.
FIGURE A-24. Virtual Analyzer Audio Options Settings Window

20. At the Audio options window, set the following:
   Uncheck **Enable Audio**.

21. On the Settings options window, click **USB**.
   The USB options are displayed.

FIGURE A-25. Virtual Analyzer USB Settings Window
22. At the USB options window, set the following:
   Uncheck **Enable USB Controller**.

23. On the Settings options window, click **Shared Folders**.
   The Shared Folders options are displayed.

![Virtual Analyzer Shared Folders Settings Window](image)

**FIGURE A-26. Virtual Analyzer Shared Folders Settings Window**

24. At the Shared Folders options window, ensure that there are no shared folders and click **OK**.
   Return to the VirtualBox Manager window.

25. At the VirtualBox Manager window, click **Start** to launch the operating system installation.
   Operating system installation is complete.

26. Set up the operating system.

**Setting up the Operating System**

**Windows 7**

1. Launch a virtual machine.
   The Install Windows 7 screen appears.
2. At the Install Windows 7 screen window, set the:
   - **Language to install** to English
   - **Time and currency format** to English (United States)
   - **Keyboard or input method** to “US”.

3. Click **Next**.
   The Windows 7 Set up screen appears.
FIGURE A-28. Window 7 Set up Screen

4. At the Windows 7 Set up screen, type:
   user name
   computer name
5. Click Next.
   The Windows 7 logon screen appears.
6. At the Windows 7 logon screen, type a password: "1111".
7. Select a password hint (required), confirm the password and click Next. The Windows 7 OS is installed.
8. After OS installation, shut down the virtual machine.

Windows XP
1. Launch a virtual machine.
   The Windows XP Professional Setup screen appears.
2. At the Windows XP Professional Setup screen, type:
   - Computer name
   - Administrator password
   - Confirm password.

3. Click Next.
   The Windows XP installation wizard opens.
4. At the Windows XP Installation Wizard type:
   Your name
5. Click Next and follow the installation wizard prompts.
   The Windows XP OS is installed.
6. After OS installation, shut down the virtual machine.
Taking a Snapshot

1. Open the Oracle VM VirtualBox Manager, highlight a virtual machine, and click the camera icon (Snapshots).

![Oracle VM VirtualBox Manager](Figure A-32)

**Figure A-32.** Oracle VM VirtualBox Manager

The snapshot screen appears.
FIGURE A-33. Snapshot Screen

2. At the snapshot screen, click the camera icon on the main menu. The Take Snapshot of Virtual Machine pop-up appears.

FIGURE A-34. Take Snapshot of Virtual Machine Pop-up

3. At the Take Snapshot of Virtual Machine pop-up, type: Snapshot name
4. Click OK.
5. Verify that a snapshot has been created.
Installing Applications

After installing the following applications, open them and accept any license agreements.

**Tip:** Do not install VBoxTool.

**Microsoft Office**

Microsoft Office 2003, 2007 and 2010 are supported.

**Note:** Microsoft Office 2003 is the environment best suited for virtual analysis.

**Adobe Acrobat Reader**

Download the most current version of Adobe Acrobat Reader:

http://www.adobe.com/downloads/
.Net Framework

For Windows XP images install .Net Framework 3.5 or later.

Download the most current version of the .Net Framework 3.5:


Note: Do not install .Net Framework on Windows 7 images; it is pre-installed on this operating system.

Configuring Automatic Login

Windows 7

1. Enable Administrator account:
   a. Run cmd
   b. Type: `net user administrator /active: yes`

2. Delete all other user accounts so that there is only one administrator account.
   a. Type: `net user "<USERNAME>" /delete`

3. Set the Administrator login password to ‘1111’.

4. Setup Automatic login
   a. `REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Administrator /f`
   b. `REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d 1111 /f`
   c. `REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f`

5. Reboot the virtual machine.

6. The virtual machine logs in automatically.

7. If auto login is unsuccessful, repeat step 4.
Windows XP

1. Delete all other user accounts so that there is only one administrator account.
   a. Type: net user "<USERNAME>" /delete

2. Set the Administrator login password to ‘1111’.

3. Setup Automatic login
   a. REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d Administrator /f
   b. REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword /t REG_SZ /d l1111 /f
   c. REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f

4. Reboot the virtual machine.

5. The virtual machine logs in automatically.

6. If auto login is unsuccessful, repeat step 4.

Using VirtualBox to Export an OVA Image

Exporting an OVA image enables the virtual machine image settings to be saved with a smaller file size and to be reused.

1. Stop the virtual machine.

2. Navigate to File > Export Appliance.
   The Appliance Export Settings Window appears.

3. Select which virtual machine to export.

Note: To be imported into Deep Discovery Inspector, the exported OVA file size must be between 10 GB and 15 GB.
4. Click **Next**. The Appliance Export Setting window appears.

5. Select a filename and location for the OVA image export.
6. Click **Next**.
   The last Appliance Export Settings window appears.

7. Double-click the description for additional configuration changes.

![Appliance Export Final Configurations Window](image)

**FIGURE A-38. Appliance Export Final Configurations Window**

8. Click **Export**.
   The OVA image export starts.

![Disk Image Export Progress Bar](image)

**FIGURE A-39. Disk Image Export Progress Bar**

The OVA export finishes.

9. Upload the OVA image file into Deep Discovery Inspector as a Virtual Analyzer.

10. Copy the OVA image file path and go to *Uploading Virtual Machine Images to Deep Discovery Inspector and Configuring Virtual Analyzer* on page A-43.
Using VirtualBox to Mount and Verify VMDK

This section explains how to use the converted image (VMDK) to create a new image in VirtualBox.

1. Open VirtualBox.
2. Click New.
   
   The Create New Virtual Machine wizard window appears.
3. Click Next.
   
   The VM Name and OS Type window appears.
4. Type the name of the VMDK along with its software and hardware configuration.
5. Click Next.
   The Memory window appears.
6. At the Memory window, use the slider to select 512 MB base memory size.
7. Click **Next**.
   The Virtual Hard Disk window appears.

8. **Select** Use existing hard disk and the converted VMDK image.

![Virtual Hard Disk Window](image)

**FIGURE A-43. Virtual Hard Disk Window**

9. Click **Next**.
   The Create New Virtual Machine Summary window appears.
10. Click **Create**.

   A new image is created and available from the VirtualBox Manager.

11. Right-click the new virtual machine and navigate to **Settings > System**.
12. In the Motherboard tab, verify the following:
   Chipset: ICH9
   Extend Features: mark **Enable IO APIC**
13. Click **OK**.
   The window closes.

14. Launch the converted VMDK to verify that it boots normally before uploading it as a Deep Discovery Inspector Virtual Analyzer.

15. See VirtualBox Manager for the status of the image.

**FIGURE A-46. VirtualBox System Settings Window**
FIGURE A-47. VirtualBox Manager
Creating a Custom Virtual Analyzer

Uploading Virtual Machine Images to Deep Discovery Inspector and Configuring Virtual Analyzer

This section explains how to:

- upload/import the OVA/VMDK image into Deep Discovery Inspector
- configure the Virtual Analyzer in Deep Discovery Inspector.

**Note:** The OVA/VMDK must be uploaded to an HTTP or FTP server prior to configuring Deep Discovery Inspector Virtual Analyzer settings. Deep Discovery Inspector can also connect via secure HTTP.

**Note:** An OVA/VMDK disk image can only be imported once into Deep Discovery Inspector. For every Virtual Analyzer in Deep Discovery Inspector, a new image file must be created using VirtualBox, to ensure that each UUID is unique.

1. Launch and log onto the Deep Discovery Inspector web console.
2. Navigate to **Administrator > Global Settings > Import Custom Virtual Analyzer**.
3. At the **Import Custom Virtual Analyzer** screen, select the following information:
   - **URL**: Use the HTTP/FTP server where the OVA/VMDK image is uploaded.
   - **User name**: If the file requires a user name/password to download, type it.
   - **Password**: If the file needs user name/password to download, please type it.
   - **Anonymous Login**: For FTP server using.

   **Note:** If the HTTP server does not require a username/password, leave these fields empty; do not enable Anonymous Login.

4. Click **Import**.
   The import completes.
FIGURE A-48. Deep Discovery Inspector Import Virtual Analyzer

5. To enable a virtual analyzer, go to Virtual Analyzer Settings on page 6-47.
Troubleshooting

The Found New Hardware Wizard opens with the image on VirtualBox

The hardware wizard automatically runs whenever an image is transferred from one machine to another. It will not affect the Virtual Analyzer.

The converted VMware VMDK displays the blue screen “Cannot find Operating System” when powered on via VirtualBox

The Chipset ICH9 must be selected and the IP APIC must be enabled.

A VMware OVA is experiencing some problems uploading into Deep Discovery Inspector

Use the VMware Converter Tool to convert the image using VirtualBox. See Converting VMware Image with VMware Converter on page A-3.

The OVA is too large and cannot upload into Deep Discovery Inspector.

The OVA/VMDK image should be between 10 GB and 15 GB.
Index

A
ActiveUpdate server 5-16
Advance Threat Scan Engine 10-3
application filters 6-14
  instant messaging 6-14
  peer-to-peer 6-14
  streaming media 6-14

B
backup
  device configuration settings 6-26
  network configuration 6-12
bare metal server 3-2

C
c CHANGE PASSWORD 4-23
components
  firmware 5-12
  IntelliTrap Exception Pattern 5-12
  IntelliTrap Pattern 5-12
  Network Content Correlation Engine 1-7, 5-12
  Network Content Correlation Pattern 5-12
  Network Content Inspection Engine 1-7, 5-12
  Network Content Inspection Pattern 5-12
  Spyware Active-monitoring Pattern 5-12
  Virus Pattern 5-11
  Virus Scan Engine 1-5, 5-11
configuration settings
  device 6-26
  network 6-12
console timeout 6-25
Control Manager 6-43
console 6-46
Control Manager registration 4-9

D
default gateway 5-5
deployment
  considerations 2-2
  dual port 2-4
  mirroring trunk links 2-9
  network TAP 2-5
  redundant networks 2-7
  remote port 2-8
  single port 2-3
specific VLAN 2-7
VLAN mirroring 2-8
detection exclusion list 6-21
about 6-21
detection log query 7-55
device configuration settings
about 6-26
device information and status 4-6
diagnostic test 4-19
documentation
conventions xii
FAQs 9-6
documentation feedback 9-10
dual port monitoring 2-4
duplex mode 4-10

F
FAQs 9-2
firmware 5-12

H
heartbeat message
Threat Discovery Appliance 6-39
high network traffic usage notifications 6-6
high risk client notifications 6-3–6-5, 6-7
high risk clients 7-67
host name 5-4

I
IM 6-14
indicators
about 7-2
risk meter 7-3
installation 3-7
installation requirements 3-3
instant messaging 6-14
integration
about 6-22
Control Manager 6-43
mitigation devices 6-36
Network VirusWall Enforcer 6-22
IntelliTrap 1-6
IntelliTrap Exception Pattern 5-12
IntelliTrap Pattern 5-12
interface speed and duplex mode settings 4-10
IP address 5-4–5-5
IP address settings 5-6, 6-39
ISO file 3-2

I-2
K
Knowledge Base 9-7
known security risks notifications 7-63

L
license
   activation 5-9, 8-2
   renewal 5-9, 8-2
logs
   about 7-55
   detection log query 7-55
   detection logs 7-55
   syslog server settings 7-65
   system 7-55
   system log query 7-64

M
mitigation devices 6-36
monitored networks 6-9
multi-layered files 1-6
multi-packed files 1-6

N
network configuration
   about 6-8
      detection exclusion list 6-21
      monitored networks 6-9
      registered domains 6-10
      network configuration settings
         about 6-12
         export 6-12
      network content correlation
         engine 5-12
         pattern 5-12
      network content inspection
         engine 5-12
         pattern 5-12
      network settings
         default gateway format 5-5
         host name format 5-4
         IP address format 5-4–5.5
         subnet mask format 5-5
         VLAN ID format 5-5
      Network Time Protocol 5-8
      network virus scan 1-7
      notifications
         about 6-2
         high network traffic usage 6-6
         high risk clients 6-3–6-5, 6-7
         known security risks 7-63
NTP 5-8
number of incidents
about 7-67

O
offline monitoring 1-7
Outbreak Containment Services 6-13

P
P2P 6-14
password 4-23, 5-3
pattern file 5-11
peer-to-peer 6-14
potential risk file 1-7
preconfiguration console 4-2, 8-3
changing root password 4-23
device information and status 4-6
import configuration file 4-13
import HTTPS certificates 4-18
interface speed and duplex mode settings 4-10
log off 4-23
overview 4-4
rollback 4-12
system logs 4-22
system tasks 4-11
protocol
support 1-8
proxy settings 5-8, 6-26

R
register
Trend Micro Control Manager 4-9
registered domains 6-10
registration
Threat Management Services Portal 6-40
Report Notification Settings 7-67
reports
about 7-66
high risk clients 7-67
number of incidents 7-67
rescue mode 8-3
rescuing the device 8-3
restarting the device 4-20
risk meter 7-3
rollback update 4-12
root password 4-23

S
Security Information Center 9-7
single port monitoring 2-3
smart protection technology 6-15
Spyware Active-monitoring Pattern 5-12
streaming media 6-14
subnet mask 5-5
suspicious files 9-9
syslog server settings 7-65
system log query 7-64
system logs 4-22
system requirements 3-3
system time settings 5-8
system updates 6-33

T
threat detections
about 6-13
block traffic 6-13
Outbreak Containment Services 6-13
Threat Discovery Appliance
about 1-2
installation 3-7
monitoring
dual port monitoring 2-4
single port monitoring 2-3
Threat Discovery Appliance components 5-11
Threat Discovery Appliance rescue tool 8-6
timeout 6-25
TMCM 6-43
true file type 1-6

U
update settings 5-13
updates
about 5-11
ActiveUpdate server 5-16
firmware 6-32
manual 5-13-5-14
scheduled 5-13, 5-15
settings 5-13
source 5-15
Using Reports 7-68

V
virtual machine 3-2
Virus Pattern 5-11
Virus Scan Engine 1-5, 5-11
VLAN ID 5-5
VMware ESX/ESXi server 6-17

W
web console timeout 6-25
web reputation 6-15
what’s new 1-3