TREND MICRO™
Deep Discovery™
Email Inspector
Installation and Deployment Guide
Advanced Protection Against Targeted Email Threats
This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp
Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Deep Discovery Email Inspector collects and provides detailed instructions on how to disable the specific features that feedback the information.


Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy
# Table of Contents

## Preface
- Preface .................................................................................................................. v
- Documentation .................................................................................................. vi
- Audience ............................................................................................................ vii
- Document Conventions .................................................................................. vii
- About Trend Micro ......................................................................................... viii

## Chapter 1: Introduction
- About Deep Discovery Email Inspector ............................................................ 1-2
- What's New ..................................................................................................... 1-2

## Chapter 2: Deployment
- Deployment Overview ................................................................................... 2-2
- Network Topology Considerations ................................................................. 2-2
  - BCC Mode ............................................................................................... 2-3
  - MTA Mode .............................................................................................. 2-4
  - SPAN/TAP Mode .................................................................................. 2-5
  - Apex Central Deployment .................................................................... 2-7
- Recommended Network Environment .......................................................... 2-8
- Items to Prepare ............................................................................................. 2-9

## Chapter 3: Installation
- System Requirements ..................................................................................... 3-2
  - Hardware Host Appliance Requirements ................................................. 3-2
  - Virtual Host Appliance Requirements ..................................................... 3-2
  - Requirements to Access Deep Discovery Email Inspector .................. 3-4
- Integrated Trend Micro Products ................................................................. 3-5
- Ports Used by the Appliance ......................................................................... 3-5
Deep Discovery Email Inspector Installation ............................................ 3-9
  Installing Deep Discovery Email Inspector on a Hardware Appliance ............................................................................................... 3-10
  Installing Deep Discovery Email Inspector on a Virtual Appliance .................................................................................................................. 3-16
Configuring Management Console Access ........................................... 3-19
Opening the Management Console ......................................................... 3-21

Chapter 4: Using the Command Line Interface

Using the CLI .................................................................................................. 4-2
Entering the CLI ............................................................................................. 4-2
Command Line Interface Commands ......................................................... 4-3
  Entering Privileged Mode ..................................................................... 4-3
  CLI Command Reference ..................................................................... 4-4

Chapter 5: Upgrading Deep Discovery Email Inspector

System Updates ............................................................................................... 5-2
Managing Patches ........................................................................................... 5-2
Upgrading Firmware ...................................................................................... 5-3
Backing Up or Restoring a Configuration .................................................. 5-5
  License Compatibility ............................................................................ 5-6

Chapter 6: Creating a New Virtual Appliance

Creating a VMWare ESXi Virtual Appliance ............................................. 6-2
  Configuring the VMware ESXi Server Network .................................... 6-2
  Creating a Virtual Machine in VMware ESXi .................................. 6-5
  Creating a Virtual Machine in Microsoft Hyper-V .......................... 6-10

Chapter 7: Technical Support

Troubleshooting Resources ........................................................................ 7-2
  Using the Support Portal ....................................................................... 7-2
  Threat Encyclopedia .............................................................................. 7-2
Table of Contents

Contacting Trend Micro ................................................................. 7-3
  Speeding Up the Support Call ...................................................... 7-4
Sending Suspicious Content to Trend Micro ................................. 7-4
  Email Reputation Services ......................................................... 7-4
  File Reputation Services ............................................................ 7-5
  Web Reputation Services ............................................................ 7-5
Other Resources ............................................................................. 7-5
  Download Center ....................................................................... 7-5
  Documentation Feedback .......................................................... 7-6

Index

Index .................................................................................................. IN-1
Preface

Topics include:

- *Documentation on page vi*
- *Audience on page vii*
- *Document Conventions on page vii*
- *About Trend Micro on page viii*
The documentation set for Deep Discovery Email Inspector includes the following:

**TABLE 1. Product Documentation**

<table>
<thead>
<tr>
<th>DOCUMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator’s Guide</td>
<td>PDF documentation provided with the product or downloadable from the Trend Micro website. The Administrator’s Guide contains detailed instructions on how to deploy, configure and manage Deep Discovery Email Inspector, and provides explanations on Deep Discovery Email Inspector concepts and features.</td>
</tr>
<tr>
<td>Installation and Deployment Guide</td>
<td>PDF documentation provided with the product or downloadable from the Trend Micro website. The Installation and Deployment Guide discusses requirements and procedures for installing and deploying Deep Discovery Email Inspector.</td>
</tr>
<tr>
<td>Syslog Content Mapping Guide</td>
<td>The Syslog Content Mapping Guide contains information on event logging formats supported by Deep Discovery Email Inspector.</td>
</tr>
<tr>
<td>Quick Start Card</td>
<td>The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Email Inspector to your network and on performing the initial configuration.</td>
</tr>
<tr>
<td>Readme</td>
<td>The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.</td>
</tr>
<tr>
<td>Online Help</td>
<td>Web-based documentation that is accessible from the Deep Discovery Email Inspector management console. The Online Help contains explanations of Deep Discovery Email Inspector components and features, as well as procedures needed to configure Deep Discovery Email Inspector.</td>
</tr>
</tbody>
</table>
Support Portal

The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website:

http://esupport.trendmicro.com

View and download Deep Discovery Email Inspector documentation from the Trend Micro Documentation Center:


Audience

The Deep Discovery Email Inspector documentation is written for IT administrators and security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, including the following topics:

- Network topologies
- Email routing
- SMTP

The documentation does not assume the reader has any knowledge of sandbox environments or threat event correlation.

Document Conventions

The documentation uses the following conventions:
### TABLE 2. Document Conventions

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UPPER CASE</strong></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, and options</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>References to other documents</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Sample command lines, program code, web URLs, file names, and program output</td>
</tr>
<tr>
<td><strong>Navigation &gt; Path</strong></td>
<td>The navigation path to reach a particular screen</td>
</tr>
<tr>
<td></td>
<td>For example, <strong>File &gt; Save</strong> means, click <strong>File</strong> and then click <strong>Save</strong> on the interface</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Configuration notes</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Recommendations or suggestions</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>Information regarding required or default configuration settings and product limitations</td>
</tr>
<tr>
<td><strong>WARNING!</strong></td>
<td>Critical actions and configuration options</td>
</tr>
</tbody>
</table>

### About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.
As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

http://www.trendmicro.com

Trend Micro and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.
Chapter 1

Introduction

Topics include:

• About Deep Discovery Email Inspector on page 1-2
• What's New on page 1-2
About Deep Discovery Email Inspector

Deep Discovery Email Inspector stops sophisticated targeted attacks and cyber threats by scanning, simulating, and analyzing suspicious links and attachments in email messages before they can threaten your network. Designed to integrate into your existing email network topology, Deep Discovery Email Inspector can act as a Mail Transfer Agent in the mail traffic flow or as an out-of-band appliance silently monitoring your network for cyber threats and unwanted spam messages.

What's New

Table 1-1. New Features in Deep Discovery Email Inspector 3.6

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MITRE ATT&amp;CK™ Framework Tactics and Techniques information</td>
<td>Deep Discovery Email Inspector includes MITRE ATT&amp;CK™ Framework Tactics and Techniques information in analysis reports.</td>
</tr>
<tr>
<td>Email Encryption</td>
<td>Email Encryption allows Deep Discovery Email Inspector to perform the following tasks based on policy settings:</td>
</tr>
<tr>
<td></td>
<td>• Decrypt messages encrypted using Trend Micro Identity-Based Encryption (IBE) for scanning</td>
</tr>
<tr>
<td></td>
<td>• Encrypt messages for secure delivery in MTA mode</td>
</tr>
<tr>
<td>Enhanced email submission</td>
<td>Deep Discovery Email Inspector supports MSG sample files for email submissions.</td>
</tr>
<tr>
<td>Enhanced policy settings</td>
<td>You can configure policies in Deep Discovery Email Inspector to scan messages based on the message direction (inbound, outbound, or inbound or outbound).</td>
</tr>
<tr>
<td></td>
<td>Deep Discovery Email Inspector determines the direction of a message using the internal domain list that you configure.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Internal domain list</td>
<td>The internal domain list allows Deep Discovery Email Inspector to determine the message direction for policies.</td>
</tr>
</tbody>
</table>
| Deep Discovery Director 5.1 support | Deep Discovery Email Inspector supports integration with Deep Discovery Director 5.1 to enable the following:  
• Central management of file passwords and Email Encryption settings  
• Synchronization of file SHA-1, file SHA-256, and URL suspicious objects  
• Server port configuration for Deep Discovery Director registration  
Deep Discovery Email Inspector also sends logs with email encryption results, and YARA rule detection and message direction information to Deep Discovery Director for central reporting. |
| Enhanced Virtual Analyzer | The Virtual Analyzer has been enhanced to include the following features:  
• New file types (.mht, .com, and .ics) for sandbox analysis  
• Windows 10 RS4, RS5, and Enterprise 2019 LTSC image support  
• Microsoft Office 2019 application support in Virtual Analyzer images  
• URL submission filtering |
| Enhanced YARA rule feature | The enhanced YARA rule feature includes the following on the Detections screens:  
• YARA detection information  
• YARA rule file name and YARA rule name filtering |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved detection capability</td>
<td>Deep Discovery Email Inspector provides increased protection by improving its detection capabilities. This release supports the following:</td>
</tr>
<tr>
<td></td>
<td>• Executable object removal from Microsoft Office files for file sanitation</td>
</tr>
<tr>
<td></td>
<td>• File SHA-256 suspicious objects for message scanning</td>
</tr>
<tr>
<td></td>
<td>• Virtual Analyzer submission priority setting for threat policy rules</td>
</tr>
<tr>
<td>File password export</td>
<td>Deep Discovery Email Inspector allows you to export all file passwords to your computer.</td>
</tr>
<tr>
<td>New action for unscannable</td>
<td>For unscannable messages that are quarantined, you can set Deep Discovery Email Inspector to open password-protected attachments using specified</td>
</tr>
<tr>
<td>messages</td>
<td>passwords and perform threat scans on messages.</td>
</tr>
<tr>
<td>New alert notification</td>
<td>Deep Discovery Email Inspector provides a new alert notification for unsuccessful message encryption and decryption.</td>
</tr>
<tr>
<td>Management console session</td>
<td>Deep Discovery Email Inspector allows you to configure the default session timeout for the management console.</td>
</tr>
<tr>
<td>timeout</td>
<td></td>
</tr>
<tr>
<td>Inline migration support</td>
<td>Deep Discovery Email Inspector provides users with the option of automatically migrating the settings from the following versions to 3.6:</td>
</tr>
<tr>
<td></td>
<td>• Deep Discovery Email Inspector 3.5</td>
</tr>
<tr>
<td></td>
<td>• Deep Discovery Email Inspector 3.2</td>
</tr>
<tr>
<td></td>
<td>• Deep Discovery Email Inspector 3.1</td>
</tr>
</tbody>
</table>
Chapter 2

Deployment

Topics include:

- Deployment Overview on page 2-2
- Network Topology Considerations on page 2-2
- Recommended Network Environment on page 2-8
- Items to Prepare on page 2-9
Deployment Overview

The following procedure provides an overview for planning the deployment and installing Deep Discovery Email Inspector.

---

Note

If you are migrating from an older version of Deep Discovery Email Inspector, see the Upgrading Firmware topic in the Deep Discovery Email Inspector Administrator's Guide for the version of Deep Discovery Email Inspector that is currently deployed.

---

Procedure

1. Decide the deployment mode.
   
   See Network Topology Considerations on page 2-2.

2. Review the system requirements.
   
   See System Requirements on page 3-2.

3. Install Deep Discovery Email Inspector.
   
   See Installing Deep Discovery Email Inspector on a Hardware Appliance on page 3-10.

4. Configure the Deep Discovery Email Inspector network settings and access the management console.
   
   See the Get Started chapter of the Deep Discovery Email Inspector Administrator's Guide.

---

Network Topology Considerations

Deploy Deep Discovery Email Inspector between the firewall or an edge Message Transfer Agent (MTA) and the network's internal mail servers.

Make sure that the management interface eth0 (on the back of the appliance) is accessible via TCP port 22 for the Command Line Interface (SSH) and TCP port 443 for the management console (HTTPS).
BCC Mode

While in BCC mode, Deep Discovery Email Inspector acts as an out-of-band appliance that does not interfere with network traffic. Deep Discovery Email Inspector discards all replicated email messages after they are checked for threats. No replicated email messages are delivered to the recipients.

Use BCC mode to understand how Deep Discovery Email Inspector processes email messages and identifies risks before fully deploying the product as an MTA. Configure an upstream MTA to mirror email traffic and handle message delivery. Deep Discovery Email Inspector sends alert notifications whenever a suspicious email message passes through the network, but does not deliver email messages.

The following figure shows how an email message passes through a network with Deep Discovery Email Inspector deployed in BCC mode. The email message enters the network and routes through the anti-spam gateway. The anti-spam gateway sends the email message through the network to the recipient and sends a copy of the email message to Deep Discovery Email Inspector. Deep Discovery Email Inspector investigates and then discards the email message.

![Figure 2-1. BCC Mode](image)
MTA Mode

While in MTA mode, Deep Discovery Email Inspector serves as a Message Transfer Agent (MTA) in the line of the mail traffic flow.

You can deploy Deep Discovery Email Inspector as an edge or non-edge MTA.

When Deep Discovery Email Inspector is deployed as a non-edge MTA in a network, an email message enters the network and routes through the relay MTA to Deep Discovery Email Inspector. The following figure shows an example.

![MTA Mode Diagram](image)

**Figure 2-2. Non-edge MTA**
When you deploy Deep Discovery Email Inspector as an edge MTA in your email network, Deep Discovery Email Inspector receives email messages from a routing gateway and performs the user-defined actions on detected messages.

![Diagram of Edge MTA](image)

**Figure 2-3. Edge MTA**

If the email message passes inspection, Deep Discovery Email Inspector routes the email message to downstream MTAs. Based on the policy configuration, Deep Discovery Email Inspector performs user-configured actions on messages that detected as spam or graymail, contain malicious file attachments, embedded URLs, content violations, or suspicious message characteristics. Deep Discovery Email Inspector then notifies recipients.

**SPAN/TAP Mode**

While in SPAN/TAP mode, Deep Discovery Email Inspector acts as an out-of-band appliance that does not interfere with network traffic. Deep Discovery Email Inspector discards all replicated email messages after they are checked for threats. No replicated email messages are delivered to the recipients.
Configure a switch or network tap to send mirrored traffic to Deep Discovery Email Inspector. Deep Discovery Email Inspector sends alert notifications whenever a suspicious email message passes through the network, but does not deliver email messages.

The following figure shows how an email message passes through a network with Deep Discovery Email Inspector deployed in SPAN/TAP mode. The email message enters the network and routes through the switch or network tap. The switch or network tap sends the email message through the network to the recipient and sends a copy of the email message to Deep Discovery Email Inspector. Deep Discovery Email Inspector investigates and then discards the email message.

![Figure 2-4. SPAN/TAP Mode](image)
Note

Deep Discovery Email Inspector virtual appliances installed in Microsoft Hyper-V do not support SPAN/TAP mode.

Apex Central Deployment

In a network topology containing multiple Deep Discovery Email Inspector appliances, Apex Central can aggregate log and suspicious objects data, generate reports, and update product components. Optionally single sign-on (SSO) through Apex Central to the management console of any registered Deep Discovery Email Inspector appliance.

The following figure shows how email messages pass through a network with multiple Deep Discovery Email Inspector appliances configured in MTA mode and registered to
Apex Central. Each Deep Discovery Email Inspector appliance independently processes email messages as an MTA while management is centralized through Apex Central.

**Figure 2-5. Apex Central Deployment**

For details about configuring Apex Central settings, see *Deep Discovery Email Inspector Administrator's Guide*.

**Recommended Network Environment**

Deep Discovery Email Inspector requires connection to a **management network**. After deployment, administrators can perform configuration tasks from any computer on the management network.
Connection to a custom network is recommended to simulate malware behavior when connecting to the Internet. For best results, Trend Micro recommends an Internet connection without proxy settings, proxy authentication, and connection restrictions.

The networks must be independent of each other so that malicious objects in the custom network do not affect entities in the management network.

Typically, the management network is the organization’s Intranet, while the custom network is an environment isolated from the Intranet, such as a test network with Internet connection.

## Items to Prepare

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Code</td>
<td>Obtain from Trend Micro</td>
</tr>
<tr>
<td>Monitor and VGA cable</td>
<td>Connects to the VGA port of the appliance</td>
</tr>
<tr>
<td>USB keyboard</td>
<td>Connects to a USB port of the appliance</td>
</tr>
<tr>
<td>USB mouse</td>
<td>Connects to a USB port of the appliance</td>
</tr>
<tr>
<td>Ethernet cables</td>
<td>Connect to the management and data ports</td>
</tr>
<tr>
<td></td>
<td>• Required: Management port (eth0) of the appliance to the management network</td>
</tr>
<tr>
<td></td>
<td>• Recommended: Data port (eth1, eth2, or eth3) connects to the custom network</td>
</tr>
<tr>
<td></td>
<td>• Optional: Unused data ports connect to the mail network for mail routing and monitoring</td>
</tr>
<tr>
<td>Requirement</td>
<td>Details</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Internet-enabled computer</td>
<td>Access to the management console from a computer with the following software installed: A supported web browser: • Microsoft Internet Explorer® 9, 10, 11 • Microsoft Edge™ • Google Chrome™ 66 or later • Mozilla Firefox® 59 or later</td>
</tr>
<tr>
<td>IP addresses</td>
<td>• Required: One IPv4 address in the management network • Recommended: One IPv4 address for the custom network • Optional: Two IPv4 addresses for the mail network and one IPv6 address for the management network</td>
</tr>
<tr>
<td>Third party software licenses</td>
<td>Licenses for all third party software installed on sandbox images</td>
</tr>
</tbody>
</table>
Chapter 3

Installation

Topics include:

• System Requirements on page 3-2
• Ports Used by the Appliance on page 3-5
• Installing Deep Discovery Email Inspector on a Hardware Appliance on page 3-10
System Requirements

This section includes the following requirements information for Deep Discovery Email Inspector:

- Hardware Host Appliance Requirements on page 3-2
- Virtual Host Appliance Requirements on page 3-2
- Requirements to Access Deep Discovery Email Inspector on page 3-4

Hardware Host Appliance Requirements

You can deploy Deep Discovery Email Inspector as a hardware appliance or virtual appliance in your network. Trend Micro provides the Deep Discovery Email Inspector appliance hardware. No other hardware is supported.

Deep Discovery Email Inspector is a self-contained, purpose-built, and performance-tuned Linux operating system. A separate operating system is not required.

Virtual Host Appliance Requirements

Deep Discovery Email Inspector supports installation on VMware ESXi 6.0 or 6.5, Microsoft Hyper-V on Windows Server 2012R2 or 2016. Deep Discovery Email Inspector virtual appliances do not support nested virtual machines.

---

**Note**

For file or URL sandbox analysis, connect Deep Discovery Email Inspector virtual appliances to Deep Discovery Analyzer.

---

Trend Micro recommends the following minimum specifications based on your licensed model’s throughput.
**Table 3-1. Specifications for Virtual Appliance**

<table>
<thead>
<tr>
<th>Messages Per Day</th>
<th>Virtual CPUs*</th>
<th>Virtual Memory (GB)</th>
<th>Virtual Disk</th>
<th>Virtual NICs**</th>
<th>Deep Discovery Analyzer 1100 Appliance***</th>
</tr>
</thead>
<tbody>
<tr>
<td>300K</td>
<td>3</td>
<td>10</td>
<td>500 GB</td>
<td>Refer to the following table</td>
<td>1 per 2 Deep Discovery Email Inspector virtual appliances</td>
</tr>
<tr>
<td>700K</td>
<td>6</td>
<td>16</td>
<td>1 TB</td>
<td>Refer to the following table</td>
<td>1 for each Deep Discovery Email Inspector virtual appliance</td>
</tr>
</tbody>
</table>

The following table shows the minimum virtual NIC requirements for each operation mode.

**Table 3-2. Minimum virtual NIC requirements**

<table>
<thead>
<tr>
<th>Operation Mode</th>
<th>Virtual NICs Required**</th>
<th>Virtual NICs Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCC</td>
<td>1</td>
<td>• ETH0 (data/management port)</td>
</tr>
<tr>
<td>MTA</td>
<td>1</td>
<td>• ETH0 (data/management port)</td>
</tr>
<tr>
<td>SPAN/TAP</td>
<td>3</td>
<td>• ETH0 (management port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ETH1 (reserved)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ETH2 (data port)</td>
</tr>
</tbody>
</table>
**Note**

* The virtual CPUs require a minimum speed of 2.3 GHz with hyper-threading support, Virtualization Technology (VT), and 64-bit architecture.

** Virtual NICs require a minimum speed of 1000 Mb/s. Trend Micro supports only the VMXNET 3 network adapter on ESXi. If you configure more than three virtual NICs for the virtual appliance, only the last two ports can be used for SPAN/TAP mode.

***Trend Micro recommends configuring two Virtual Analyzer images with 60 instances on a Deep Discovery Analyzer 1100 appliance to analyze up to 16000 samples per day.

### Requirements to Access Deep Discovery Email Inspector

The following table lists the minimum requirements to access the Command Line Interface and the management console that manage Deep Discovery Email Inspector.

**Table 3-3. System Access Requirements**

<table>
<thead>
<tr>
<th>APPLICATION</th>
<th>REQUIREMENTS</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH client</td>
<td>SSH protocol version 2</td>
<td>Set the Command Line Interface terminal window size to 80 columns and 24 rows.</td>
</tr>
<tr>
<td>Internet Explorer™</td>
<td>Versions 9, 10, 11</td>
<td>Use only a supported browser to access the management console.</td>
</tr>
<tr>
<td>Microsoft Edge™</td>
<td>Windows 10</td>
<td>Using the data port IP address you set during the initial configuration, specify the following URL:</td>
</tr>
<tr>
<td>Mozilla Firefox™</td>
<td>Version 59 or later</td>
<td>https://[Appliance_IP_Address]:443</td>
</tr>
<tr>
<td>Google Chrome™</td>
<td>Version 66 or later</td>
<td></td>
</tr>
</tbody>
</table>
Note

• Trend Micro recommends viewing the console using a monitor that supports 1280 x 1024 resolution or greater.

• By default, SSH service is disabled and is not started when enabled. To enable SSH service, see configure service ssh enable on page 4-12. To start SSH service, see start service ssh on page 4-26.

Integrated Trend Micro Products

For seamless integration, make sure that the Trend Micro products that integrate with Deep Discovery Email Inspector run the required or recommended versions.

**TABLE 3-4. Trend Micro Products and Services that Integrate with Deep Discovery Email Inspector**

<table>
<thead>
<tr>
<th>PRODUCT/ SERVICE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep Discovery Director</td>
<td>• 5.1</td>
</tr>
<tr>
<td>Deep Discovery Analyzer</td>
<td>• 6.8</td>
</tr>
<tr>
<td></td>
<td>• 6.5</td>
</tr>
<tr>
<td>Apex Central</td>
<td>• 2019</td>
</tr>
<tr>
<td>Control Manager</td>
<td>• 7.0 with the latest hotfix installed</td>
</tr>
<tr>
<td>Smart Protection Server</td>
<td>• 3.3</td>
</tr>
<tr>
<td></td>
<td>• 3.2</td>
</tr>
<tr>
<td>TippingPoint Security Management System (SMS)</td>
<td>• 5.3</td>
</tr>
<tr>
<td></td>
<td>• 5.2</td>
</tr>
</tbody>
</table>

Ports Used by the Appliance

The following table shows the ports that are used with Deep Discovery Email Inspector and why they are used.
### Table 3-5. Ports used by Deep Discovery Email Inspector

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>FUNCTION</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>Listening</td>
<td>Endpoints connect to Deep Discovery Email Inspector through SSH.</td>
</tr>
<tr>
<td>25</td>
<td>TCP</td>
<td>Listening</td>
<td>MTAs and mail servers connect to Deep Discovery Email Inspector through SMTP.</td>
</tr>
<tr>
<td>53</td>
<td>TCP/UDP</td>
<td>Outbound</td>
<td>Deep Discovery Email Inspector uses this port for:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DNS resolution</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Sender authentication (SPF, DKIM, DMARC) query</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Listening and outbound</td>
<td>Deep Discovery Email Inspector connects to other computers and integrated Trend Micro products and hosted services through this port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Connect to the Customer Licensing Portal to manage the product licenses</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Query Community File Reputation Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Query Community Domain/IP Reputation Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Query Web Reputation Services through the Smart Protection Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Upload virtual analyzer images to Deep Discovery Email Inspector using the image import tool</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Communicate with Trend Micro Apex Central if Deep Discovery Email Inspector is registered over HTTP</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Function</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>Outbound</td>
<td>Deep Discovery Email Inspector connects to the NTP server to synchronize time.</td>
</tr>
<tr>
<td>161</td>
<td>TCP</td>
<td>Listening</td>
<td>Deep Discovery Email Inspector uses this port to listen for requests from SNMP managers.</td>
</tr>
<tr>
<td>162</td>
<td>TCP</td>
<td>Outbound</td>
<td>Deep Discovery Email Inspector connects to SNMP managers to send SNMP trap messages.</td>
</tr>
<tr>
<td><strong>PORT</strong></td>
<td><strong>PROTOCOL</strong></td>
<td><strong>FUNCTION</strong></td>
<td><strong>PURPOSE</strong></td>
</tr>
<tr>
<td>----------</td>
<td>--------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 443      | TCP          | Listening and outbound | Deep Discovery Email Inspector uses this port to:  
• Query Predictive Machine Learning engine  
• Query Web Inspection Service  
• Access the management console with a computer through HTTPS  
• Communicate with Trend Micro Apex Central  
• Connect to the Smart Protection Network and query Web Reputation Services  
• Connect to Trend Micro Threat Connect  
• Send anonymous threat information to Smart Feedback  
• Update components by connecting to the ActiveUpdate server  
• Send product usage information to Trend Micro feedback servers  
• Verify the safety of files through the Certified Safe Software Service  
• Communicate with Deep Discovery Director  
• Share threat intelligence information and exception list with other products |
| 636      | TCP          | Outbound     | Deep Discovery Email Inspector uses this port as the default port to connect to the Microsoft Active Directory server for third-party authentication. |
### Deep Discovery Email Inspector Installation

Deep Discovery Email Inspector is available as a hardware or virtual appliance.

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>FUNCTION</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>3269</td>
<td>TCP</td>
<td>Outbound</td>
<td>Deep Discovery Email Inspector uses this port as the default port to connect to the Microsoft Active Directory server for LDAP query using Global Catalog.</td>
</tr>
<tr>
<td>4459</td>
<td>TCP</td>
<td>Listening and outbound</td>
<td>Endpoints connect to the End-User Quarantine console on Deep Discovery Email Inspector through this port.</td>
</tr>
<tr>
<td>5274</td>
<td>TCP</td>
<td>Outbound</td>
<td>Deep Discovery Email Inspector uses this port as the default port to connect to the Smart Protection Server for web reputation services.</td>
</tr>
</tbody>
</table>
| User-defined | N/A  | Outbound | Deep Discovery Email Inspector uses specified ports to:  
  • Send logs to syslog servers  
  • Share threat intelligence with integrated products/services  
  • Upload detection logs to SFTP servers  
  • Communicate with Check Point Open Platform for Security (OPSEC) |
Trend Micro provides two server models with Deep Discovery Email Inspector pre-installed. After you have received your Deep Discovery Email Inspector appliance, configure network settings using the Command Line Interface (CLI) to gain access to the management console.

For more information, see Configuring Management Console Access on page 3-19.

### Virtual appliance

Deep Discovery Email Inspector supports installation on VMware ESXi 6.0 or 6.5, and Microsoft Hyper-V on Windows Server 2012R2 or 2016.

For more information, see Virtual Host Appliance Requirements on page 3-2.

---

### Installing Deep Discovery Email Inspector on a Hardware Appliance

**Important**

The Deep Discovery Email Inspector appliance comes with the appliance software installed. The following procedure provides a reference for fresh installs only.

Trend Micro provides the Deep Discovery Email Inspector appliance hardware. No other hardware is supported. For information about software requirements, see System Requirements on page 3-2.

**WARNING!**

The installation deletes any existing data or partitions on the selected disk. Back up existing data before installing Deep Discovery Email Inspector.

**Procedure**

1. Power on the server.

2. Insert the Deep Discovery Email Inspector Installation DVD into the optical disc drive.
3. Restart the server.

4. The server boots from the Deep Discovery Email Inspector Installation DVD and the installation begins. Select **Install Appliance**.

   ![Deep Discovery Email Inspector Installation](image)

   After the setup initializes, the **License Agreement** screen appears.

5. Click **Accept**.
6. Select the device to install Deep Discovery Email Inspector.
7. Click \textbf{Continue}.

8. At the warning message, click \textbf{Yes} to continue.

The Deep Discovery Email Inspector installer scans the hardware to determine that it meets the minimum specifications.

9. Click \textbf{Next}.

The \textbf{Summary} screen appears.

10. Click \textbf{Continue} to begin the installation.
11. At the warning message, click **Continue**.
After formatting the disk, the program installs the operating system. The Deep Discovery Email Inspector appliance installs after the appliance restarts.

12. Remove the Installation DVD from the optical disc drive to prevent reinstallation.

13. Configure network settings to access the management console.

   For details, see *Configuring Management Console Access on page 3-19*.

14. Open the management console.

   For details, see *Opening the Management Console on page 3-21*.

   For information about configuring Deep Discovery Email Inspector, see the *Deep Discovery Email Inspector Administrator’s Guide*. 
Installing Deep Discovery Email Inspector on a Virtual Appliance

WARNING!
Back up any existing data on the target hard disk before installing Deep Discovery Email Inspector. The installation process formats and repartitions the hard disk and removes all existing data.

Important
- You must separately license VMware ESXi and such use is subject to the terms and conditions of the VMware license agreement for that product.
- Deleting an eth port on the Deep Discovery Email Inspector virtual appliance requires reinstallation.

Procedure
1. Create a virtual appliance.
   For details, see Creating a New Virtual Appliance on page 6-1.
   When installing Deep Discovery Email Inspector on a VMware ESXi server, disable the snapshot feature for the virtual appliance to preserve hard disk space.
2. Start the virtual machine.
3. Perform the following tasks:
   a. Insert the Deep Discovery Email Inspector installation DVD into the physical CD/DVD drive of the hypervisor server.
   b. Connect the virtual CD/DVD drive of the virtual appliance to the physical CD/DVD drive of the hypervisor server.
   c. Connect the virtual CD/DVD drive of the virtual appliance to the ISO file.
4. Restart the virtual appliance.
a. In the VMware vSphere Client, go to **Virtual Machine** > [virtual machine name].

b. Click **Console** and select **Open browser console**.

c. On the console screen that appears, click **Actions** on the top-left corner and click **Guest OS > Send keys > Ctrl-Alt-Delete**.

The installation screen appears.

5. Select **Install Appliance** and press ENTER. Then, follow the procedure in *Installing Deep Discovery Email Inspector on a Hardware Appliance on page 3-10* to complete the installation process.

6. (Optional) Remove the DVD to prevent reinstallation.

7. Configure network settings to access the management console.

   For details, see *Configuring Management Console Access on page 3-19*.

8. Open the management console.

   For details, see *Opening the Management Console on page 3-21*.

   For information about configuring Deep Discovery Email Inspector, see the *Deep Discovery Email Inspector Administrator's Guide*. 
Setting Options for Virtual Appliance in ESXi 6.x

Configure settings in ESXi to enable Deep Discovery Email Inspector management console navigation.

Procedure

1. Go to VMware ESXi > Virtual Machines, and right-click the appliance name and select Edit Settings....

   The settings screen appears.

2. On the Settings screen, click the VM Options tab and select VMware Tools.

3. Disable the Synchronize guest time with host option.
After completing the installation, the server restarts and loads the Command Line Interface (CLI). Configure Deep Discovery Email Inspector network settings to gain access to the management console.

The following procedure explains how to log on to the CLI and configure the following required network settings:

- Management IP address and netmask
• Host name
• DNS
• Gateway

Procedure

1. Log on to the CLI with the default credentials.
   • User name: admin
   • Password: ddei

2. At the prompt, type `enable` and press Enter to enter privileged mode.

3. Type the default password, `trend#1`, and then press Enter.
   The prompt changes from > to #.

4. Configure network settings with the following command:
   ```
   configure network basic
   ```

5. Configure the following network settings and press Enter after typing each setting.

   **Note**
   IPv6 settings are optional.

   • Host name
   • IPv4 address
   • Subnet mask
   • IPv4 gateway
   • Preferred IPv4 DNS
   • Alternate IPv4 DNS
   • IPv6 address
Installation

• Prefix length
• IPv6 gateway
• Preferred IPv6 DNS
• Alternate IPv6 DNS

6. Type Y to confirm settings and restart.

Deep Discovery Email Inspector implements specified network settings and then restarts all services.

The initial configuration is complete and the management console is accessible.

Opening the Management Console

Deep Discovery Email Inspector provides a built-in management console that you can use to configure and manage the product.

View the management console using any supported web browser. For information about supported browsers, see System Requirements on page 3-2.

For information about configuring required network settings before accessing the management console, see Configuring Management Console Access on page 3-19.

Procedure

1. In a web browser, type the IP address of the Deep Discovery Email Inspector server in the format https://<Appliance IP Address>.

    Note
    The default management console IP address / subnet mask is 192.168.252.1 / 255.255.0.0.

The logon screen appears.
2. Specify the logon credentials (user name and password).

   **Note**
   Use the default administrator logon credentials when logging on for the first time:
   - User name: **admin**
   - Password: **ddei**

3. Click **Log On**.

   The management console **Dashboard** appears.

   **Important**
   Trend Micro recommends changing the password after logging on to the management console for the first time.

   For details, see the *Deep Discovery Email Inspector Administrator's Guide*. 
Chapter 4

Using the Command Line Interface

Topics include:

• Using the CLI on page 4-2
• Entering the CLI on page 4-2
• Command Line Interface Commands on page 4-3
Using the CLI

Use the Command Line Interface (CLI) to perform the following tasks:

- Configure initial settings, such as the device IP address and host name
- Restart the device
- View device status
- Debug and troubleshoot the device

---

**Note**

Do not enable scroll lock on your keyboard when using HyperTerminal. If scroll lock is enabled, you cannot enter data.

---

Entering the CLI

To log on to the CLI, either connect directly to the server or connect using SSH.

---

**Procedure**

- To connect directly to the server:
  
  a. Connect a monitor and keyboard to the server.
  
  b. Log on to the CLI.

---

**Note**

The default credentials are:

- User name: admin
- Password: ddei

- If the SSH service is enabled, do the following to connect using SSH:
a. Verify the computer you are using can ping Deep Discovery Email Inspector’s IP address.

b. Use an SSH client to connect to Deep Discovery Email Inspector’s IP address and TCP port 22.

---

**Note**

The default IP address / subnet mask is 192.168.252.1 / 255.255.0.0.

---

**Command Line Interface Commands**

The Deep Discovery Email Inspector CLI commands are separated into two categories: normal and privileged commands. Normal commands are basic commands to obtain system information and to perform simple tasks. Privileged commands provide full configuration control and advanced monitoring and debugging features. Privileged commands are protected by the `enable` command and password.

**Entering Privileged Mode**

---

**WARNING!**

Enter the shell environment only if your support provider instructs you to perform debugging operations.

---

**Procedure**

1. Log on to the CLI.
   
   See *Entering the CLI on page 4-2*.

2. At the prompt, type `enable` and press ENTER to enter privileged mode.

3. Type the default password, `trend#1`, and then press ENTER.
The prompt changes from > to #.

---

**CLI Command Reference**

The following tables explain the CLI commands.

---

**Note**

CLI commands require privileged mode. For details, see *Entering Privileged Mode on page 4-3*.

---

**configure product management-port**

**TABLE 4-1. configure product management-port**

<table>
<thead>
<tr>
<th>View</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax:</td>
<td>configure product management-port [ipv4</td>
</tr>
<tr>
<td>ipv4</td>
<td>Configure IPv4 settings</td>
</tr>
<tr>
<td>ipv6</td>
<td>Configure IPv6 settings</td>
</tr>
<tr>
<td>&lt;ip&gt;</td>
<td>IP address for the interface</td>
</tr>
<tr>
<td>&lt;mask&gt;</td>
<td>Network mask for the NIC</td>
</tr>
</tbody>
</table>

**Example:**

To set the management port IPv4 address:

```
configure product management-port ipv4 192.168.10.21 255.255.255.0
```
configure product operation-mode

TABLE 4-2. configure product operation-mode

Set the Deep Discovery Email Inspector operation mode

| Syntax: | configure product operation-mode [BCC | MTA | TAP] |
|---------|---------------------------------------------|
| View    | Privileged                                 |
| Parameters | BCC: Deploy in BCC mode  
|         | MTA: Deploy in MTA mode  
|         | TAP: Deploy in SPAN/TAP mode                |

Example:

To deploy in BCC mode:

configure product operation-mode BCC

configure network basic

TABLE 4-3. configure network basic

Configures basic network settings, including host name, IP address, subnet mask, gateway, and DNS.

<table>
<thead>
<tr>
<th>Syntax:</th>
<th>configure network basic</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Privileged</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Examples:</td>
<td></td>
</tr>
</tbody>
</table>
***Network Configuration***

Specify value for each item and press ENTER. Settings apply to the management port (Eth0) and require a restart.

Host name: mail.com
IPv4 address: 10.64.70.151
Subnet mask: 255.255.254.0
IPv4 gateway: 10.64.70.1
Preferred IPv4 DNS: 10.64.1.55
Alternate IPv4 DNS: 10.64.1.54
IPv6 address:
Prefix length:
IPv6 gateway:
Preferred IPv6 DNS:
Alternate IPv6 DNS:
Confirm changes and restart (Y/N):

---

`configure network dns`

**TABLE 4-4. configure network dns**

| Configures DNS settings for the Deep Discovery Email Inspector device. |
|-----------------------------|-----------------------------|
| **Syntax:**                |                             |
| `configure network dns [ipv4 | ipv6] <dns1> <dns2>`             |                             |
| **View**                   | Privileged                  |
### Parameters

<table>
<thead>
<tr>
<th><strong>ipv4</strong></th>
<th>Configure IPv4 settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ipv6</strong></td>
<td>Configure IPv6 settings</td>
</tr>
<tr>
<td><strong>&lt;dns1&gt;</strong></td>
<td>Primary DNS server</td>
</tr>
<tr>
<td><strong>&lt;dns2&gt;</strong></td>
<td>Secondary DNS server</td>
</tr>
</tbody>
</table>

**Note**

Use a space to separate the primary and secondary DNS value.

### Examples:

To configure the primary DNS with an IP address of 192.168.10.21:

```plaintext
configure network dns ipv4 192.168.10.21
```

To configure the primary and secondary DNS with the following values:

- Primary DNS: 192.168.10.21
- Secondary DNS: 192.168.10.22

```plaintext
configure network dns ipv4 192.168.10.21 192.168.10.22
```

### configure network hostname

**Table 4-5. configure network hostname**

Configures the host name for the Deep Discovery Email Inspector device.

**Syntax:**

```plaintext
configure network hostname <hostname>
```

<table>
<thead>
<tr>
<th><strong>View</strong></th>
<th><strong>Privileged</strong></th>
</tr>
</thead>
</table>

| **Parameters** | **<hostname>**: The host name or fully qualified domain name (FQDN) for the Deep Discovery Email Inspector device |

**Examples:**
To change the host name of the Deep Discovery Email Inspector device to test.host.com:

```
configure network hostname test.example.com
```

### configure network interface

**TABLE 4-6. configure network interface**

Configures the IP address for the network interface card (NIC).

**Syntax:**

```
configure network interface [ipv4 | ipv6] <interface> <ip> <mask>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>ipv4: Configure IPv4 settings</td>
</tr>
<tr>
<td></td>
<td>ipv6: Configure IPv6 settings</td>
</tr>
<tr>
<td></td>
<td><code>&lt;interface&gt;</code>: NIC name</td>
</tr>
<tr>
<td></td>
<td><code>&lt;ip&gt;</code>: IP address for the interface</td>
</tr>
<tr>
<td></td>
<td><code>&lt;mask&gt;</code>: Network mask for the NIC</td>
</tr>
</tbody>
</table>

**Example:**

To configure an NIC with the following values:

- **Interface:** eth0
- **IPv4 address:** 192.168.10.10
- **IPv4 subnet mask:** 255.255.255.0

```
configure network interface ipv4 eth0 192.168.10.10 255.255.255.0
```

### configure network route add

**TABLE 4-7. configure network route add**

Adds a new route entry
**Syntax:**

```
configure network route add [ipv4 | ipv6] <ip_prefixlen> <via> <dev>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameters</strong></td>
<td></td>
</tr>
<tr>
<td><strong>ipv4</strong></td>
<td>Configure IPv4 settings</td>
</tr>
<tr>
<td><strong>ipv6</strong></td>
<td>Configure IPv6 settings</td>
</tr>
<tr>
<td><code>&lt;ip_prefixlen&gt;</code>: Destination network ID with format IP_Address/Prefixlen</td>
<td></td>
</tr>
<tr>
<td><code>&lt;via&gt;</code>: IP address of the next hop</td>
<td></td>
</tr>
<tr>
<td><code>&lt;dev&gt;</code>: Device name</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

To add a new route entry:

```
configure network route add ipv4 172.10.10.0/24 192.168.10.1 eth1
```

**configure network route default**

**Table 4-8. configure network route default**

<table>
<thead>
<tr>
<th>Sets the default route</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>configure network route default [ipv4</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td><strong>ipv4</strong></td>
</tr>
<tr>
<td><strong>ipv6</strong></td>
</tr>
<tr>
<td><code>&lt;gateway&gt;</code>: IP address of default gateway</td>
</tr>
</tbody>
</table>

**Example:**

To set the default route for the Deep Discovery Email Inspector appliance:

```
configure network route default ipv4 192.168.10.1
```
**configure network route del**

**TABLE 4-9. configure network route del**

<table>
<thead>
<tr>
<th>Deletes a route</th>
</tr>
</thead>
</table>

**Syntax:**

configure network route del [ipv4 | ipv6] <ip_prefixlen> <via> <dev>

**View** | Privileged
---|---

**Parameters**

- ipv4: Configure IPv4 settings
- ipv6: Configure IPv6 settings
- <ip_prefixlen>: Destination network ID with format IP_Address/Prefixlen
- <via>: IPv4 address of the next hop
- <dev>: Device name

**Example:**

To delete a route for the Deep Discovery Email Inspector appliance:

configure network route del ipv4 172.10.10.0/24 192.168.10.1 eth1

**configure network route del default/default ipv6**

**TABLE 4-10. configure network route del default/default ipv6**

<table>
<thead>
<tr>
<th>Deletes the default IPv6 gateway</th>
</tr>
</thead>
</table>

**Syntax:**

configure network route del default ipv6 <gateway> <device>

**View** | Privileged
---|---

**Parameters**

- gateway: IPv6 Address of the default gateway
- device: Link local to IPv6 default gateway
Example:

To delete the default IPv6 gateway fe80::20c:29ff:fe75:b579 on device eth0: `configure network route del default ipv6 fe80::20c:29ff:fe75:b579 eth0`

**configure service nscd disable**

<table>
<thead>
<tr>
<th>TABLE 4-11. configure service nscd disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the name service cache daemon (nscd) at system startup.</td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>configure service nscd disable</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To disable the name service cache daemon at system startup:</td>
</tr>
<tr>
<td><code>configure service nscd disable</code></td>
</tr>
</tbody>
</table>

**configure service nscd enable**

<table>
<thead>
<tr>
<th>TABLE 4-12. configure service nscd enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables the name service cache daemon (nscd) at system startup.</td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>configure service nscd enable</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To enable the name service cache daemon at system startup:</td>
</tr>
<tr>
<td><code>configure service nscd enable</code></td>
</tr>
</tbody>
</table>
### configure service ssh disable

**TABLE 4-13. configure service ssh disable**

<table>
<thead>
<tr>
<th>Enables SSH on all network interface cards (NIC).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>configure service ssh disable</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To disable SSH on all NICs:</td>
</tr>
<tr>
<td><code>configure service ssh disable</code></td>
</tr>
</tbody>
</table>

### configure service ssh enable

**TABLE 4-14. configure service ssh enable**

<table>
<thead>
<tr>
<th>Enables SSH on one specific network interface card (NIC).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td><code>configure service ssh enable</code></td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>None</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To enable SSH:</td>
</tr>
<tr>
<td><code>configure service ssh enable</code></td>
</tr>
</tbody>
</table>
### configure service ssh port

**TABLE 4-15. configure service ssh port**

<table>
<thead>
<tr>
<th>Change SSH service port.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>configure service ssh port &lt;port&gt;</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>port: configure the SSH service port</td>
</tr>
<tr>
<td>&lt;port&gt;: SSH service port number</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>To change the SSH service port to 56743: configure service ssh port 56743</td>
</tr>
</tbody>
</table>

### configure service ntp

**TABLE 4-16. configure service ntp**

<table>
<thead>
<tr>
<th>Synchronize the Deep Discovery Email Inspector system time with an NTP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>configure service ntp [enable</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>enable: Enable NTP</td>
</tr>
<tr>
<td>disable: Disable NTP</td>
</tr>
<tr>
<td>server-address: Configure the NTP server address</td>
</tr>
<tr>
<td>&lt;address&gt;: Specify the FQDN or IP address of the NTP server</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td>To configure the NTP server address as 192.168.10.21:</td>
</tr>
<tr>
<td>configure service ntp server-address 192.168.10.21</td>
</tr>
</tbody>
</table>
To enable synchronization with the NTP server:

```
configure service ntp enable
```

### configure system date

**TABLE 4-17. configure system date**

| Configures the time and date and saves the data in CMOS. |

<table>
<thead>
<tr>
<th>Syntax:</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure system date &lt;date&gt; &lt;time&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>&lt;date&gt;: Set the date using the following format: <code>yyyy-mm-dd</code></td>
</tr>
<tr>
<td></td>
<td>&lt;time&gt;: Set the time with the following format: <code>hh:mm:ss</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>To set the date to August 12, 2010 and the time to 3:40 PM:</td>
</tr>
<tr>
<td>configure system date 2010-08-12 15:40:00</td>
</tr>
</tbody>
</table>

### configure system password enable

**TABLE 4-18. configure system password enable**

| To change the password required to enter Privileged mode. |

<table>
<thead>
<tr>
<th>Syntax:</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure system password enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
</tbody>
</table>

| Examples: |
To change the password required to enter Privileged mode:
```
configure system password enable
```

**configure system timezone**

**TABLE 4-19. configure system timezone**

Configures the time zone used by Deep Discovery Email Inspector.

**Syntax:**
```
configure system timezone <region> <city>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
</table>
| Parameters | <region>: Region name  
|          | <city>: City name |

**Example:**

To configure the Deep Discovery Email Inspector appliance to use the time zone for the following location:

Region: America  
City: New York
```
configure system timezone America New_York
```

**TABLE 4-20. Time Zone Setting Examples**

<table>
<thead>
<tr>
<th>REGION/COUNTRY</th>
<th>CITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>Cairo</td>
</tr>
<tr>
<td></td>
<td>Harare</td>
</tr>
<tr>
<td></td>
<td>Nairobi</td>
</tr>
<tr>
<td>REGION/COUNTRY</td>
<td>CITY</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>America</td>
<td>Anchorage</td>
</tr>
<tr>
<td></td>
<td>Bogota</td>
</tr>
<tr>
<td></td>
<td>Buenos_Aires</td>
</tr>
<tr>
<td></td>
<td>Caracas</td>
</tr>
<tr>
<td></td>
<td>Chicago</td>
</tr>
<tr>
<td></td>
<td>Chihuahua</td>
</tr>
<tr>
<td></td>
<td>Denver</td>
</tr>
<tr>
<td></td>
<td>Godthab</td>
</tr>
<tr>
<td></td>
<td>Lima</td>
</tr>
<tr>
<td></td>
<td>Los_Angeles</td>
</tr>
<tr>
<td></td>
<td>Mexico_City</td>
</tr>
<tr>
<td></td>
<td>New_York</td>
</tr>
<tr>
<td></td>
<td>Noronha</td>
</tr>
<tr>
<td></td>
<td>Phoenix</td>
</tr>
<tr>
<td></td>
<td>Santiago</td>
</tr>
<tr>
<td></td>
<td>St_Johns</td>
</tr>
<tr>
<td></td>
<td>Tegucigalpa</td>
</tr>
<tr>
<td>REGION/COUNTRY</td>
<td>CITY</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Asia</td>
<td>Almaty</td>
</tr>
<tr>
<td></td>
<td>Baghdad</td>
</tr>
<tr>
<td></td>
<td>Baku</td>
</tr>
<tr>
<td></td>
<td>Bangkok</td>
</tr>
<tr>
<td></td>
<td>Calcutta</td>
</tr>
<tr>
<td></td>
<td>Colombo</td>
</tr>
<tr>
<td></td>
<td>Dhaka</td>
</tr>
<tr>
<td></td>
<td>Hong_Kong</td>
</tr>
<tr>
<td></td>
<td>Irkutsk</td>
</tr>
<tr>
<td></td>
<td>Jerusalem</td>
</tr>
<tr>
<td></td>
<td>Kabul</td>
</tr>
<tr>
<td></td>
<td>Karachi</td>
</tr>
<tr>
<td></td>
<td>Katmandu</td>
</tr>
<tr>
<td></td>
<td>Krasnoyarsk</td>
</tr>
<tr>
<td></td>
<td>Kuala_Lumpur</td>
</tr>
<tr>
<td></td>
<td>Kuwait</td>
</tr>
<tr>
<td></td>
<td>Magadan</td>
</tr>
<tr>
<td></td>
<td>Manila</td>
</tr>
<tr>
<td></td>
<td>Muscat</td>
</tr>
<tr>
<td></td>
<td>Rangoon</td>
</tr>
<tr>
<td></td>
<td>Seoul</td>
</tr>
<tr>
<td></td>
<td>Shanghai</td>
</tr>
<tr>
<td>Region/Country</td>
<td>City</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Asia (Continued)</td>
<td>Singapore</td>
</tr>
<tr>
<td></td>
<td>Taipei</td>
</tr>
<tr>
<td></td>
<td>Tehran</td>
</tr>
<tr>
<td></td>
<td>Tokyo</td>
</tr>
<tr>
<td></td>
<td>Yakutsk</td>
</tr>
<tr>
<td>Atlantic</td>
<td>Acores</td>
</tr>
<tr>
<td>Australia</td>
<td>Adelaide</td>
</tr>
<tr>
<td></td>
<td>Brisbane</td>
</tr>
<tr>
<td></td>
<td>Darwin</td>
</tr>
<tr>
<td></td>
<td>Hobart</td>
</tr>
<tr>
<td></td>
<td>Melbourne</td>
</tr>
<tr>
<td></td>
<td>Perth</td>
</tr>
<tr>
<td>Europe</td>
<td>Amsterdam</td>
</tr>
<tr>
<td></td>
<td>Athens</td>
</tr>
<tr>
<td></td>
<td>Belgrade</td>
</tr>
<tr>
<td></td>
<td>Berlin</td>
</tr>
<tr>
<td></td>
<td>Brussels</td>
</tr>
<tr>
<td></td>
<td>Bucharest</td>
</tr>
<tr>
<td></td>
<td>Dublin</td>
</tr>
<tr>
<td></td>
<td>Moscow</td>
</tr>
<tr>
<td></td>
<td>Paris</td>
</tr>
</tbody>
</table>
### enable

**Table 4-21. enable**

<table>
<thead>
<tr>
<th>Region/Country</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pacific</td>
<td>Auckland</td>
</tr>
<tr>
<td></td>
<td>Fiji</td>
</tr>
<tr>
<td></td>
<td>Guam</td>
</tr>
<tr>
<td></td>
<td>Honolulu</td>
</tr>
<tr>
<td></td>
<td>Kwajalein</td>
</tr>
<tr>
<td></td>
<td>Midway</td>
</tr>
<tr>
<td>US</td>
<td>Alaska</td>
</tr>
<tr>
<td></td>
<td>Arizona</td>
</tr>
<tr>
<td></td>
<td>Central</td>
</tr>
<tr>
<td></td>
<td>East-Indiana</td>
</tr>
<tr>
<td></td>
<td>Eastern</td>
</tr>
<tr>
<td></td>
<td>Hawaii</td>
</tr>
<tr>
<td></td>
<td>Mountain</td>
</tr>
<tr>
<td></td>
<td>Pacific</td>
</tr>
</tbody>
</table>

Enters privileged mode so privileged commands can be provided.

**Syntax:**

```
enable
```

**View**

Normal

**Parameters**

None

**Example:**
To enter privileged mode:

```
enable
```

### exit

**TABLE 4-22. exit**

<table>
<thead>
<tr>
<th>Description</th>
<th>Syntax</th>
<th>Parameters</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exits privileged mode.</td>
<td><code>exit</code></td>
<td>None</td>
<td>To exit privileged mode or to exit the session when not in privileged mode:</td>
</tr>
<tr>
<td>Exits the session for those not in privileged mode.</td>
<td></td>
<td></td>
<td><code>exit</code></td>
</tr>
</tbody>
</table>

### help

**TABLE 4-23. help**

<table>
<thead>
<tr>
<th>Description</th>
<th>Syntax</th>
<th>Parameters</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the CLI help information.</td>
<td><code>help</code></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
To display the CLI help information:

```
help
```

### history

**TABLE 4-24. history**

<table>
<thead>
<tr>
<th>Displays the current session's command line history.</th>
<th></th>
</tr>
</thead>
</table>

**Syntax:**

```
history [limit]
```

**View** | Normal
---|---

**Parameters**

* [limit]: Specifies the size of the history list for the current session

Specifying "0" retains all commands for the session.

**Example:**

To specify six commands for the size of the history list:

```
history 6
```

### logout

**TABLE 4-25. logout**

<table>
<thead>
<tr>
<th>Logs out of the current CLI session.</th>
<th></th>
</tr>
</thead>
</table>

**Syntax:**

```
logout
```

**View** | Normal
---|---

**Parameters** | None
---|---

**Example:**

```
To logout from the current session:
logout

### ping

**TABLE 4-26. ping**

<table>
<thead>
<tr>
<th>View</th>
<th>Parameters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>[c num_echos]</strong>: Specifies the number of echo requests to be sent. Default value is 5.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>[i interval]</strong>: Specifies the delay interval in seconds between each packet. Default value is 1 second.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>&lt;dest&gt;</strong>: Specifies the destination host name or IP address</td>
<td></td>
</tr>
</tbody>
</table>

**Syntax:**

```
ping [-c num_echos] [-i interval] <dest>
```

**Examples:**

To ping the IP address 192.168.1.1:
```
ping 192.168.1.1
```

To ping the host remote.host.com:
```
ping remote.host.com
```

### ping6

**TABLE 4-27. ping6**

<table>
<thead>
<tr>
<th>View</th>
<th>Parameters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>[c num_echos]</strong>: Specifies the number of echo requests to be sent. Default value is 5.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>[i interval]</strong>: Specifies the delay interval in seconds between each packet. Default value is 1 second.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>&lt;dest&gt;</strong>: Specifies the destination host name or IP address</td>
<td></td>
</tr>
</tbody>
</table>

**Syntax:**

```
ping6 [-c num_echos] [-i interval] <dest>
```
### Using the Command Line Interface

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
</table>
| Parameters | `-c num_echos`: Specifies the number of echo requests to be sent. Default value is 5.  
`[-i interval]`: Specifies the delay interval in seconds between each packet. Default value is 1 second.  
<dest>: Specifies the destination host name or IP address |

#### Examples:

To ping the IPv6 address `fe80::21a:a5ff:fec1:1060`:
```
ping6 fe80::21a:a5ff:fec1:1060
```

To ping the host `remote.host.com`:
```
ping6 remote.host.com
```

---

#### start task postfix drop

**TABLE 4-28. start task postfix drop**

Deletes a specified message or all messages in the email message queue.

**Syntax:**
```
start task postfix drop { <mail_id> | all }
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td><code>&lt;mail_id&gt;</code>: Specifies the message ID in the postfix queue to delete</td>
</tr>
</tbody>
</table>

**Examples:**

To delete email message `D10D4478A5` from the email message queue:
```
start task postfix drop D10D4478A5
```

To delete all email messages from the email message queue:
```
start task postfix drop all
```
**start task postfix flush**

**TABLE 4-29. start task postfix flush**

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempts to deliver all queued email messages.</td>
<td></td>
</tr>
</tbody>
</table>

**Syntax:**

\[
\text{start task postfix flush}
\]

**View** | Privileged  
**Parameters** | None  

**Example:**

To deliver all queued email messages:

\[
\text{start task postfix flush}
\]

**start task postfix queue**

**TABLE 4-30. start task postfix queue**

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays all email messages queued in Postfix.</td>
<td></td>
</tr>
</tbody>
</table>

**Syntax:**

\[
\text{start task postfix queue}
\]

**View** | Privileged  
**Parameters** | None  

**Example:**

To display all Postfix queued email messages:

\[
\text{start task postfix queue}
\]
### start service nscd

**TABLE 4-31. start service nscd**

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Starts the name service cache daemon (nscd).</td>
<td></td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
<td>start service nscd</td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>To start the name service cache daemon:</td>
<td>start service nscd</td>
</tr>
</tbody>
</table>

### start service postfix

**TABLE 4-32. start service postfix**

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Starts the Postfix mail system</td>
<td></td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
<td>start service postfix</td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>To start the Postfix mail system:</td>
<td>start service postfix</td>
</tr>
</tbody>
</table>
### start service product

**TABLE 4-33. start service product**

<table>
<thead>
<tr>
<th>Start the Product service system.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
<td></td>
</tr>
<tr>
<td><code>start service product</code></td>
<td></td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>To start the Product service system:</td>
<td></td>
</tr>
<tr>
<td><code>start service product</code></td>
<td></td>
</tr>
</tbody>
</table>

### start service ssh

**TABLE 4-34. start service ssh**

<table>
<thead>
<tr>
<th>Starts the ssh service system.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
<td></td>
</tr>
<tr>
<td><code>start service ssh</code></td>
<td></td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>To start the ssh service system:</td>
<td></td>
</tr>
<tr>
<td><code>start ssh service</code></td>
<td></td>
</tr>
</tbody>
</table>
**stop process core**

**TABLE 4-35. stop process core**

<table>
<thead>
<tr>
<th>Description</th>
<th>Stops a running process and generates a core file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>stop process core <code>&lt;pid&gt;</code></td>
</tr>
<tr>
<td>View</td>
<td>Privileged</td>
</tr>
<tr>
<td>Parameters</td>
<td><code>&lt;pid&gt;</code>: The process ID</td>
</tr>
<tr>
<td>Example</td>
<td>To stop a process with ID 33:</td>
</tr>
<tr>
<td></td>
<td><code>stop process core 33</code></td>
</tr>
</tbody>
</table>

**stop service nscd**

**TABLE 4-36. stop service nscd**

<table>
<thead>
<tr>
<th>Description</th>
<th>Stops the name service cache daemon (nscd).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>stop service nscd</td>
</tr>
<tr>
<td>View</td>
<td>Privileged</td>
</tr>
<tr>
<td>Parameters</td>
<td>None</td>
</tr>
<tr>
<td>Example</td>
<td>To stop the name service cache daemon:</td>
</tr>
<tr>
<td></td>
<td><code>stop service nscd</code></td>
</tr>
</tbody>
</table>
stop service postfix

**TABLE 4-37. stop service postfix**

<table>
<thead>
<tr>
<th>Stops the Postfix mail system.</th>
</tr>
</thead>
</table>

**Syntax:**

```
stop service postfix
```

**View**  | Privileged
---|---
**Parameters** | None

**Example:**

To stop the Postfix mail system:

```
stop service postfix
```

stop service product

**TABLE 4-38. stop service product**

<table>
<thead>
<tr>
<th>Stops the Product service system.</th>
</tr>
</thead>
</table>

**Syntax:**

```
stop service product
```

**View**  | Privileged
---|---
**Parameters** | None

**Example:**

To stop the Product service system:

```
stop service product
```
stop service ssh

**TABLE 4-39. stop service ssh**

<table>
<thead>
<tr>
<th>Stops the ssh service system.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong> stop service ssh</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
</tbody>
</table>

reboot

**TABLE 4-40. reboot**

<table>
<thead>
<tr>
<th>Reboots the Deep Discovery Email Inspector appliance immediately or after a specified delay.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong> reboot [time]</td>
</tr>
<tr>
<td><strong>View</strong></td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
resolve

**TABLE 4-41. resolve**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolves an IPv4 address from a host name or resolves a host name from an IPv4 address.</td>
<td></td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
<td></td>
</tr>
<tr>
<td><code>resolve &lt;dest&gt;</code></td>
<td></td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Privileged</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
<td><code>&lt;dest&gt;</code>: Specifies the IPv4 address or host name to resolve</td>
</tr>
<tr>
<td><strong>Examples:</strong></td>
<td></td>
</tr>
<tr>
<td>To resolve the host name from IP address 192.168.10.1:</td>
<td></td>
</tr>
<tr>
<td><code>resolve 192.168.10.1</code></td>
<td></td>
</tr>
<tr>
<td>To resolve the IP address from host name parent.host.com:</td>
<td></td>
</tr>
<tr>
<td><code>resolve parent.host.com</code></td>
<td></td>
</tr>
</tbody>
</table>

show storage statistic

**TABLE 4-42. show storage statistic**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the file system disk space usage.</td>
<td></td>
</tr>
<tr>
<td><strong>Syntax:</strong></td>
<td></td>
</tr>
<tr>
<td><code>show storage statistic [partition]</code></td>
<td></td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Normal</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td><code>[partition]</code>: Specify a partition. This is optional.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>To display the file system disk space usage of the Deep Discovery Email Inspector appliance:</td>
<td></td>
</tr>
<tr>
<td><code>show storage statistic</code></td>
<td></td>
</tr>
</tbody>
</table>
### show network

**TABLE 4-43. show network**

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameters</strong></td>
<td></td>
</tr>
<tr>
<td><strong>arp</strong></td>
<td>Displays the value returned by the Address Resolution Protocol (ARP) for the given address.</td>
</tr>
<tr>
<td><strong>&lt;address&gt;</strong></td>
<td>FQDN or IP address that will be resolved with the Address Resolution Protocol (ARP).</td>
</tr>
<tr>
<td><strong>connections</strong></td>
<td>Displays the current network connections of the Deep Discovery Email Inspector appliance.</td>
</tr>
<tr>
<td><strong>dns</strong></td>
<td>Displays the DNS IP address of the Deep Discovery Email Inspector appliance.</td>
</tr>
<tr>
<td><strong>dns ipv6</strong></td>
<td>Displays system DNS configuration for IPv6.</td>
</tr>
<tr>
<td><strong>hostname</strong></td>
<td>Displays the host name of the Deep Discovery Email Inspector appliance.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td>Displays the network interface card (NIC) status and configuration.</td>
</tr>
<tr>
<td><strong>route</strong></td>
<td>Displays IP address route table.</td>
</tr>
<tr>
<td><strong>route ipv4</strong></td>
<td>Displays system IPv4 route table.</td>
</tr>
<tr>
<td><strong>route default ipv4</strong></td>
<td>Displays default IPv4 route table.</td>
</tr>
<tr>
<td><strong>route default ipv6</strong></td>
<td>Display default IPv6 route table.</td>
</tr>
</tbody>
</table>

**Examples:**

To display the ARP information for the address 10.2.23.41:

```
show network arp 10.2.23.41
```
To display the current network connections of the Deep Discovery Email Inspector appliance:

```
show network connections
```

To display the DNS configuration:

```
show network dns
```

To display system DNS configuration for IPv6:

```
show network dns ipv6
```

To display the host name of the Deep Discovery Email Inspector appliance:

```
show network hostname
```

To display the NIC status and configuration:

```
show network interface
```

To display the IP address route table:

```
show network route
```

To display system IPv4 route table:

```
show network route ipv4
```

To display system default IPv4 gateway:

```
show network route default ipv4
```

To display system default IPv6 gateway:

```
show network route default ipv6
```

---

**show kernel**

**TABLE 4-44. show kernel**

<table>
<thead>
<tr>
<th>Displays the OS kernel information of the Deep Discovery Email Inspector appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax:</td>
</tr>
<tr>
<td>show kernel {messages</td>
</tr>
</tbody>
</table>
Using the Command Line Interface

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>messages:</td>
<td>Displays kernel messages.</td>
</tr>
<tr>
<td>modules:</td>
<td>Displays kernel modules.</td>
</tr>
<tr>
<td>parameters:</td>
<td>Displays kernel parameters.</td>
</tr>
<tr>
<td>iostat:</td>
<td>Displays CPU statistics and I/O statistics for devices and partitions.</td>
</tr>
</tbody>
</table>

**Examples:**

To display the OS kernel’s messages:

```
show kernel messages
```

To display the OS kernel’s modules:

```
show kernel modules
```

To display the OS kernel’s parameters:

```
show kernel parameters
```

To display the CPU statistics and I/O statistics:

```
show kernel iostat
```

**show service**

**TABLE 4-45. show service**

Displays the Deep Discovery Email Inspector service status.

**Syntax:**

```
show service [ntp <enabled | server-address> | ssh | nscd]
```

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
</table>
**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nscd</td>
<td>Displays the status of the name service cache daemon.</td>
</tr>
<tr>
<td>ntp enabled</td>
<td>Displays the system NTP service status.</td>
</tr>
<tr>
<td>ntp server-address</td>
<td>Displays the system NTP service server address.</td>
</tr>
<tr>
<td>ssh</td>
<td>Displays the status of SSH.</td>
</tr>
</tbody>
</table>

**Examples:**

To display the name service cache daemon status:

```
show service nscd
```

To display the NTP service status:

```
show service ntp
```

To display the SSH status:

```
show service ssh
```

**show memory**

**TABLE 4-46. show memory**

<table>
<thead>
<tr>
<th>Displays the system memory information.</th>
</tr>
</thead>
</table>

**Syntax:**

```
show memory [vm | statistic]
```

**View**

<table>
<thead>
<tr>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
</tr>
</tbody>
</table>

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm</td>
<td>Displays virtual memory statistics</td>
</tr>
<tr>
<td>statistic</td>
<td>Displays system memory statistics</td>
</tr>
</tbody>
</table>

**Examples:**

To display the virtual memory statistics:

```
show memory vm
```
To display the system memory statistics:

```
show memory statistic
```

**show process**

**TABLE 4-47. showprocess**

Displays the status of the processes that are currently running.

**Syntax:**

```
show process [top | stack | itrace | trace] [pid]
```

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
</table>
| **Parameters** | `top`: Displays the status of the processes that are currently running and system related processes  
               `stack`: Print a stack trace of a running process  
               `itrace`: Trace the library call  
               `trace`: Trace system calls and signals  
               `pid`: The process id number |

**Examples:**

To display the status of the processes that are currently running:

```
show process
```

To display the stack trace of process 1233:

```
show process stack 1233
```

To display the system call of process 1233:

```
show process trace 1233
```

To display the library call of process 1233:

```
show process itrace 1233
```
show product-info

**TABLE 4-48. show product-info**

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>management-port:</td>
<td>Displays the management port's IP address and subnet mask</td>
</tr>
<tr>
<td>operation-mode:</td>
<td>Displays the operation mode of Deep Discovery Email Inspector</td>
</tr>
<tr>
<td>service-status:</td>
<td>Displays the status of services</td>
</tr>
<tr>
<td>version:</td>
<td>Displays the product version</td>
</tr>
</tbody>
</table>

**Examples:**

- To display the management port's IP address and mask: `show product-info management-port`
- To display the operation mode: `show product-info operation-mode`
- To display the status of the service: `show-product-info service-status`
- To display the build version of Deep Discovery Email Inspector: `show product-info version`

show system

**TABLE 4-49. show system**

<table>
<thead>
<tr>
<th>Displays various system settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax:</strong></td>
</tr>
<tr>
<td>`show system [date</td>
</tr>
</tbody>
</table>
Using the Command Line Interface

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td></td>
</tr>
<tr>
<td>date: Displays the current time and date.</td>
<td></td>
</tr>
<tr>
<td>timezone: Displays the timezone settings. You can optionally specify the timezone information to view:</td>
<td></td>
</tr>
<tr>
<td>• continent: Displays the system continent</td>
<td></td>
</tr>
<tr>
<td>• city: Displays the system city</td>
<td></td>
</tr>
<tr>
<td>• country: Displays the system country</td>
<td></td>
</tr>
<tr>
<td>uptime: Displays how long the Deep Discovery Email Inspector appliance has been running.</td>
<td></td>
</tr>
<tr>
<td>version: Displays version number for the Deep Discovery Email Inspector appliance.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples:**

To display the current time and date of the Deep Discovery Email Inspector appliance:

```
show system date
```

To display the timezone settings:

```
show system timezone
```

To display the continent of the Deep Discovery Email Inspector appliance:

```
show system timezone continent
```

To display the city of the Deep Discovery Email Inspector appliance: device's city:

```
show system timezone city
```

To display the country of the Deep Discovery Email Inspector appliance:

```
show system timezone country
```

To display how long Deep Discovery Email Inspector has been running:

```
show system uptime
```

To display the version number of the Deep Discovery Email Inspector appliance:

```
show system version
```
shutdown

**TABLE 4-50. shutdown**

<table>
<thead>
<tr>
<th>Specifies shutting down the Deep Discovery Email Inspector appliance immediately or after a specified delay.</th>
</tr>
</thead>
</table>

**Syntax:**

```
shutdown [time]
```

<table>
<thead>
<tr>
<th>View</th>
<th>Privileged</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameters</th>
<th>[time]: Shuts down the Deep Discovery Email Inspector appliance after a specified delay in minutes.</th>
</tr>
</thead>
</table>

**Examples:**

To shut down the Deep Discovery Email Inspector appliance immediately:

```
shutdown
```

To shut down the Deep Discovery Email Inspector appliance after a 5 minute delay:

```
shutdown 5
```

traceroute

**TABLE 4-51. traceroute**

<table>
<thead>
<tr>
<th>Displays the tracking route to a specified destination.</th>
</tr>
</thead>
</table>

**Syntax:**

```
traceroute [-h hops] <dest>
```

<table>
<thead>
<tr>
<th>View</th>
<th>Normal</th>
</tr>
</thead>
</table>

| Parameters | [-h hops]: Specifies the maximum number of hops to the destination. The minimum number is 6.  
<dest>: Specifies the remote system to trace |
|---|---|

**Examples:**


To display the route to IP address 172.10.10.1 with a maximum of 6 hops:

```
traceroute 172.10.10.1
```

To display the route to IP address 172.10.10.1 with a maximum of 30 hops:

```
traceroute -h 30 172.10.10.1
```
Chapter 5

Upgrading Deep Discovery Email Inspector

Topics include:

- System Updates on page 5-2
- Managing Patches on page 5-2
- Upgrading Firmware on page 5-3
- Backing Up or Restoring a Configuration on page 5-5
System Updates

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

**TABLE 5-1. System Updates**

<table>
<thead>
<tr>
<th>SYSTEM UPDATE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotfix</td>
<td>A hotfix is a workaround or solution to a single customer-reported issue. Hotfixes are issue-specific, and are not released to all customers.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>A new hotfix may include previous hotfixes until Trend Micro releases a patch.</td>
</tr>
<tr>
<td>Security patch</td>
<td>A security patch focuses on security issues suitable for deployment to all customers. Non-Windows patches commonly include a setup script.</td>
</tr>
<tr>
<td>Patch</td>
<td>A patch is a group of hotfixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis.</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 hotfix, patch, and service pack releases:


Managing Patches

From time to time, Trend Micro releases a new firmware version for a reported known issue or an upgrade that applies to the product. Find available firmware versions at [http://downloadcenter.trendmicro.com/](http://downloadcenter.trendmicro.com/).

You can install a patch file on Trend Micro using one of the following methods:
• The Deep Discovery Email Inspector management console
• Plan deployment from Deep Discovery Director. For more information, see the Deep Discovery Director documentation.

Procedure

1. Go to **Administration > Product Updates > Hotfixes / Patches**.

2. Under **History**, verify the software version number.

3. Manage the product patch.
   • Upload a patch by browsing to the patch file provided by Trend Micro Support and then clicking **Install** under **Install Hotfix / Patch**.
   • Roll back a patch by clicking **Roll Back** under **History**. After rollback, Deep Discovery Email Inspector uses the most recent previous configuration. For example, rolling back patch 3 returns Deep Discovery Email Inspector to a patch 2 state.

Upgrading Firmware

From time to time, Trend Micro releases a new firmware version for a reported known issue or an upgrade that applies to the product. Find available firmware versions at [http://downloadcenter.trendmicro.com](http://downloadcenter.trendmicro.com).

Updating the firmware ensures that Deep Discovery Email Inspector has access to new and improved security features when they become available.

You can upgrade the firmware on Deep Discovery Email Inspector using one of the following methods:

• The Deep Discovery Email Inspector management console
• Plan deployment from Deep Discovery Director. For more information, see the Deep Discovery Director documentation.
Note

Ensure that you have finished all management console tasks before proceeding. The upgrade process may take some time to complete, and upgrading from Deep Discovery Email Inspector 3.5, 3.2, or 3.1 to Deep Discovery Email Inspector 3.6 may take an hour or more. Trend Micro recommends starting the upgrade during off-peak office hours. Installing the update restarts Deep Discovery Email Inspector.

Procedure

1. Back up configuration settings.
   
   Backing Up or Restoring a Configuration on page 5-5

2. Obtain the firmware image.
   
   • Download the Deep Discovery Email Inspector firmware image from the Trend Micro Download Center at:
     
     http://downloadcenter.trendmicro.com
   
   • Obtain the firmware package from your Trend Micro reseller or support provider.

3. Save the image to any folder on a computer.

4. Go to Administration > Product Updates > Firmware.

5. Next to Software version, verify your firmware version.


7. Click Install.

   Tip

   You can access the command line interface to view the installation process.

   After the installation is complete, Deep Discovery Email Inspector automatically restarts and the command line interface appears.

8. Perform the following post-installation steps:
• Clear the browser cache.
• Manually log onto the web console.
• If Deep Discovery Email Inspector is using an internal Virtual Analyzer that connects to the Internet through a proxy server, reconfigure the proxy settings for the internal Virtual Analyzer.

## Backing Up or Restoring a Configuration

Export settings from the management console to back up the Deep Discovery Email Inspector configuration. If a system failure occurs, you can restore the settings by importing the configuration file that you previously backed up.

---

**Important**

Deep Discovery Email Inspector only supports restoring configurations from other Deep Discovery Email Inspector servers with a compatible license status and with the same firmware version, hardware model, and locale. For example, you cannot restore a server running version 3.6 with a configuration file backed up from a server running version 3.1 or earlier versions.

For more information on compatible licenses, see *License Compatibility on page 5-6*.

---

**Note**

When exporting/importing your settings, the database will be locked. Therefore, all Deep Discovery Email Inspector actions that depend on database access will not function.

---

Trend Micro recommends:

• Backing up the current configuration before each import operation
• Performing the operation when Deep Discovery Email Inspector is idle. Importing and exporting affects Deep Discovery Email Inspector performance.

Back up settings to create a copy of Deep Discovery Email Inspector appliance configuration to restore the configuration in another Deep Discovery Email Inspector...
appliance or to revert to the backup settings at a later time. Replicate a configuration across several Deep Discovery Email Inspector appliances by restoring the same configuration file into each appliance.

License Compatibility

The following table indicates compatible product licenses. You can only restore configuration files backed up from other Deep Discovery Email Inspector servers with a compatible license, and with the same firmware version, hardware model, and locale.

**TABLE 5-2. License compatibility**

<table>
<thead>
<tr>
<th>LICENSE ACTIVATION</th>
<th>ADVANCED THREAT PROTECTION + GATEWAY MODULE</th>
<th>GATEWAY MODULE ONLY</th>
<th>ADVANCED THREAT PROTECTION ONLY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ADVANCED THREAT PROTECTION + GATEWAY MODULE</strong></td>
<td>Compatible</td>
<td>Compatible</td>
<td>Compatible</td>
</tr>
<tr>
<td><strong>GATEWAY MODULE ONLY</strong></td>
<td>Not compatible</td>
<td>Compatible</td>
<td>Not compatible</td>
</tr>
<tr>
<td><strong>ADVANCED THREAT PROTECTION ONLY</strong></td>
<td>Not compatible</td>
<td>Not compatible</td>
<td>Compatible</td>
</tr>
</tbody>
</table>
Creating a New Virtual Appliance

Learn how to create a virtual appliance using VMware ESXi or Microsoft Hyper-V in the following sections:

- *Creating a VMWare ESXi Virtual Appliance on page 6-2*
- *Creating a Virtual Machine in Microsoft Hyper-V on page 6-10*

For details about the minimum virtual host appliance system requirements and supported hypervisors, see *Virtual Host Appliance Requirements on page 3-2.*
Creating a VMWare ESXi Virtual Appliance

Learn how to create a virtual appliance using VMware ESXi in the following topics:

- Configuring the VMware ESXi Server Network on page 6-2
- Creating a Virtual Machine in VMware ESXi on page 6-3

Configuring the VMware ESXi Server Network

Use a browser to connect the ESXi server.

Procedure

1. To log in to the VMware ESXi server, type a **User name** and **Password**, and then click **Log In**.
2. Click **Networking** and then click the **Virtual switches** tab. Observe the initial state.

3. Click **Add standard virtual switches** and configure the following settings.
   a. For **vSwitch Name**, type a name (for example, Management Network).
   b. For **Uplink 1**, select a NIC card for **Management Network**.
   c. **Click Add**.
4. (Optional) Add a data network. On the **Virtual switches** tab, click **Add standard virtual switches** and configure the settings.

**Note**

If Deep Discovery Email Inspector is set in SPAN/TAP mode with uplink ports to a standard virtual switch, enable promiscuous mode for the virtual switch.

a. For **vSwitch Name**, type a name.

b. For **Uplink 1**, select a NIC card for the data network.

c. Expand **Security** and select **Accept** for **Promiscuous mode**.

5. Click on the **Port groups** tab and observe the initial state.

6. Click **Add port group** and configure the following settings.

a. For **Name**, type a name (for example, Management Port Group).

b. For **VLAN ID**, type a number (for example, 1000).

c. For **Virtual switch**, select **Management Network**.

7. Click **Add**.
8. (Optional) Add a data port group.

Note

If SPAN/TAP mode is enabled, configure one additional port group.

9. In the Port groups tab, click Data port group and verify that it is connected to the Management Network.

Creating a Virtual Machine in VMware ESXi

The following procedure is for VMware.

Procedure

1. Click Virtual machines and then click Create / Register VM.

2. On the Select creation type screen, click Create a new virtual machine and then click Next.
3. On the Select a name and guest OS screen, configure the settings.
   a. For **Name**, type **New Virtual Machine**.
   b. For **Compatibility**, select **ESXi 6.5 virtual machine**.
   c. For **Guest OS family**, select **Linux**.
   d. For **Guest OS version**, select **CentOS 7 (64-bit)**.
4. Click **Next**.

5. On the **Select storage screen**, select the destination storage where the virtual machine resides and click **Next**.
6. Configure the settings on the **Customize settings** screen.

   a. For **CPU**, select the virtual CPU amount based on the throughput of your Virtual Deep Discovery Email Inspector license.
      
      - For 300K messages per day, select at least 3 virtual CPUs.
      - For 700K messages per day, select at least 6 virtual CPUs.

   b. For **Memory**, set the amount of memory based on the throughput of your Virtual Deep Discovery Email Inspector license.
      
      - For 300K messages per day, set at least 10 GB of memory for the virtual machine.
      - For 700K messages per day, select at least 16 GB of memory for the virtual machine.

   c. For **Hard disk**, set the amount of disk space based on the throughput of your Virtual Deep Discovery Email Inspector license.
      
      - For 300K messages per day, set at least 500 GB of disk space for the virtual machine.
• For 700K messages per day, select at least 1 TB of disk space for the virtual machine.

d. For Network, configure the amount of NICs based on the function of your Virtual Deep Discovery Email Inspector license.

• If Deep Discovery Email Inspector is set in MTA or BCC mode, configure at least 1 NIC.

• If SPAN/TAP mode is enabled, configure at least 3 NICs with one each for the management and data networks.

i. Set the VMware ESXi server VM Network as the Deep Discovery Email Inspector Management Network (NIC 1).

ii. Set the Data port group as the Deep Discovery Email Inspector Data Network (NIC 2).

iii. For Adapter Type, select VMXNET 3.

### Note

In VMware ESXi 6.0, select the **Thick provisioned, lazily zeroed** option for the **Disk Provisioning** field. This is the default setting in VMware ESXi 6.5.

7. Click Next.

8. On the **Ready to complete** screen, review the settings and click **Finish**.
Creating a Virtual Machine in Microsoft Hyper-V

Procedure

1. Create virtual management and data switches.
   a. In Hyper-V Manager, go to Action > Virtual Switch Manager.

The Virtual Switch Manager window appears.
b. In the left column, click **New Virtual network switch**.

   The **Create virtual switch** screen appears.

c. For the switch type to create, select **External**.
d. Click **Create Virtual Switch**.

The **Virtual Switch Properties** screen appears.

e. For **Name**, type **Management Switch**.

f. For **Connection type**, select **External Network** and then select a NIC card to use for the management network.
g. Click **Apply**.

The **Apply Networking Changes** confirmation window appears.
h. Read the warning and then click Yes.

i. In the left column, click New Virtual network switch. The Create virtual switch screen appears.

j. For the switch type to create, select External.

k. Click Create Virtual Switch. The Virtual Switch Properties screen appears.

l. For Name, type Data Switch.

m. For Connection type, select External Network and then select a NIC card to use for the data network.
n. Click **Apply**.

   The **Apply Networking Changes** confirmation window appears.

o. Read the warning and then click **Yes**.

   The confirmation window closes.

p. Click **OK**.

2. Create a virtual machine.

   a. In Hyper-V Manager, go to **Action > New > Virtual Machine**.

   ![Hyper-V Manager](image)

   The **New Virtual Machine Wizard** window with the **Before You Begin** screen appears.

   b. Click **Next**.

      The **Specify Name and Location** screen appears.
c. For **Name**, type *Deep Discovery Email Inspector*.

![Specify Name and Location](image)

- **Specify Generation** screen appears.

d. Click **Next**.

The **Specify Generation** screen appears.

e. Select **Generation 1**.
f. Click **Next**.

The **Assign Memory** screen appears.

g. For **Startup memory**, assign at least **10240 MB (10 GB)**.
h. Click **Next**.

The **Configure Networking** screen appears.

i. For **Connection**, select **Management Switch**.
j. Click **Next**.

The **Connect Virtual Hard Disk** screen appears.

k. Select **Attach a virtual hard disk later**.
1. Click **Next**.

   The **Completing the New Virtual Machine Wizard** screen appears.

m. Verify that the virtual machine configuration is correct and then click **Finish**.

3. Create a virtual hard disk.
   
a. In Hyper-V Manager, select the Deep Discovery Email Inspector virtual machine and then go to **Action > New > Hard Disk**.
b. Click **Next**.

The **Choose Disk Format** screen appears.

c. Select **VHDX**.
d. Click **Next**.

The **Choose Disk Type** screen appears.

e. Select **Fixed size**.
f. Click **Next**.

The **Specify Name and Location** screen appears.

g. For **Name**, type **Deep Discovery Email Inspector.vhdx**.
h. Click **Next**.

The **Configure Disk** screen appears.

i. Select **Create a New blank virtual hard disk**.

j. For **Size**, specify at least 500 GB.
k. Click **Next**.

The **Completing the New Virtual Hard Disk Wizard** screen appears.

l. Verify that the hard disk configuration is correct and then click **Finish**.

**Note**

Finishing may take a few minutes. Wait for the process to complete before continuing.

4. Configure the virtual machine.
   a. In Hyper-V Manager, select the Deep Discovery Email Inspector virtual machine and then go to **Action > Settings**.
The settings window appears.

b. In the left column, click **Processor**.

The **Processor** settings appear.

c. For **Number of virtual processors**, specify at least 3 virtual processors.
d. Click **Apply**.

e. In the left column, click **IDE Controller 0**.

   The **IDE Controller** settings appear.

f. For the type of hard drive to attach to the controller, select **Hard Drive**.
g. Click Add.

The **Hard Drive** settings appear.

h. For **Virtual hard disk**, specify the location of **Deep Discovery Email Inspector.vhdx**.
i. In the left column, click **IDE Controller 1** and then click on **DVD Drive**. The **DVD Drive** settings appear.

j. For **Media**, select **Image file** and then specify the location of the Deep Discovery Email Inspector ISO file.
k. In the left column, click **Add Hardware**.

The **Add Hardware** settings appear.

l. For the devices you want to add, select **Network Adapter**.
m. Click Add.

   The **Network Adapter** settings appear.

n. For **Virtual switch**, select **Data Switch**.
o. Click **Apply**.

p. Click **OK**.
Technical Support

Learn about the following topics:

- Troubleshooting Resources on page 7-2
- Contacting Trend Micro on page 7-3
- Sending Suspicious Content to Trend Micro on page 7-4
- Other Resources on page 7-5
Troubleshooting Resources

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

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

2. Select from the available products or click the appropriate button to search for solutions.
3. Use the Search Support box to search for available solutions.
4. If no solution is found, click Contact Support and select the type of support needed.

Tip
To submit a support case online, visit the following URL:


A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia
provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:

• Malware and malicious mobile code currently active or "in the wild"
• Correlated threat information pages to form a complete web attack story
• Internet threat advisories about targeted attacks and security threats
• Web attack and online trend information
• Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

| Address | Trend Micro, Incorporated  
| 225 E. John Carpenter Freeway, Suite 1500  
| Irving, Texas 75062 U.S.A. |
| Phone | Phone: +1 (817) 569-8900  
| Toll-free: (888) 762-8736 |
| Website | http://www.trendmicro.com |
| Email address | support@trendmicro.com |

• Worldwide support offices:
• Trend Micro product documentation:
  http://docs.trendmicro.com
Speeding Up the Support Call

To improve problem resolution, have the following information available:

• Steps to reproduce the problem
• Appliance or network information
• Computer brand, model, and any additional connected hardware or devices
• Amount of memory and free hard disk space
• Operating system and service pack version
• Version of the installed agent
• Serial number or Activation Code
• Detailed description of install environment
• Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:


Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

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

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.
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
Index

A
about
  deployment, 2-2
administration, 5-2, 5-3, 5-5
back up settings, 5-5
product upgrades, 5-2, 5-3
restore settings, 5-5

B
backup, 5-5

C
CLI, 4-1
command line interface
  entering the shell environment, 4-3
Command Line Interface, 4-1
  accessing, 4-2
  using, 4-2
configuration
  management console, 3-19, 3-21

D
deployment
  installation, 3-10
  network topology, 2-2
overview, 2-2
  system requirements, 3-2
documentation feedback, 7-6
Download Center, 5-2, 5-3

E
Email Encryption, 1-2
enter CLI, 4-1
Ethernet cables, 2-9
export settings, 5-5

F
firmware update, 5-3

G
getting started
  management console, 3-21
  management console access, 3-19

I
import settings, 5-5
installation, 3-2
  network topology, 2-3–2-5
  operating system, 3-10
Intranet, 2-9

M
Malware Lab Network, 2-8
management console, 3-19, 3-21
management network, 2-8
minimum requirements, 3-2

N
network environment, 2-8
network topology, 2-2

O
operation modes
  BCC mode, 2-3
  MTA mode, 2-4
  SPAN/TAP mode, 2-5

P
patches, 5-3
ports, 3-5
product upgrade, 5-2, 5-3
R
requirements, 3-2
restore, 5-5

S
shell environment, 4-3
support
resolve issues faster, 7-4
system requirements, 3-2
system updates, 5-2

T
test network, 2-9

U
using CLI, 4-1