



# 5.1 TREND MICRO<sup>™</sup> Deep Discovery<sup>™</sup> **Email Inspector** Installation and Deployment Guide











Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/home.aspx/

Trend Micro, the Trend Micro t-ball logo, Trend Micro Apex One, Trend Micro Apex Central, and Deep Discovery are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2021. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM59195/210115

Release Date: April 2021

Protected by U.S. Patent No.: Patents pending.

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 <u>docs@trendmicro.com</u>.

Evaluate this documentation on the following site:

https://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.

https://success.trendmicro.com/data-collection-disclosure

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	1
Documentation	2
Audience	3
Document Conventions	3
About Trend Micro	4

### **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	2-3
BCC Mode	2-3
MTA Mode	2-4
SPAN/TAP Mode	2-6
Apex Central Deployment	2-8
Recommended Network Environment	2-9
Items to Prepare 2	2-10

## **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 Ins	spector
3-4	
Integrated Trend Micro Products	3-5

Ports Used by the Appliance 3-
Deep Discovery Email Inspector Installation 3-
Installing Deep Discovery Email Inspector on a Hardware Appliance With an Optical Drive
Configuring Management Console Access 3-1
The Management Console 3-19
Logging On Using Local Accounts 3-19 Logging On With Single Sign-On 3-20

## Chapter 4: Using the Command Line Interface

ii

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
configure product management-port 4-4
configure product operation-mode 4-5
configure network basic 4-5
configure network dns 4-6
configure network hostname 4-7
configure network interface 4-8
configure network teaming reinit 4-8
configure network route add 4-9
configure network route default 4-9
configure network route del 4-10
configure network route del default/default ipv6 4-10
configure service nscd disable 4-11
configure service nscd enable 4-11
configure service ssh disable 4-12

iii

configure service ssh enable	4-12
configure service ssh port	4-13
configure service ntp	4-13
configure system date	4-14
configure system password enable	4-14
configure system timezone	4-15
enable	4-19
exit	4-19
help	4-20
history	4-20
logout	4-21
ping	4-21
ping6	4-22
start task postfix drop	4-22
start task postfix flush	4-23
start task postfix queue	4-23
start service nscd	4-24
start service postfix	4-24
start service product	4-25
start service ssh	4-25
stop process core	4-25
stop service nscd	4-26
stop service postfix	4-26
stop service product	4-27
stop service ssh	4-27
reboot	4-28
resolve	4-28
show storage statistic	4-29
show network	4-29
show kernel	4-31
show service	4-32
show memory	4-33
show process	4-33
show product-info	4-34
show system	4-35
shutdown	4-36
traceroute	4-37

### **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 Creating a Virtual Machine in VMware ESXi	6-2 6-5
Creating a Virtual Machine in Microsoft Hyper-V	6-9
Creating a Virtual Machine using KVM	. 6-31
Creating a Virtual Machine on Nutanix AHV	. 6-38

### **Chapter 7: Technical Support**

Troubleshooting Resources	7-2
Using the Support Portal Threat Encyclopedia	7-2 7-2
Contacting Trend Micro	7-3
Speeding Up the Support Call	7-4
Sending Suspicious Content to Trend Micro	7-4
Email Reputation Services File Reputation Services Web Reputation Services	7-4 7-5 7-5
Other Resources	7-5
Download Center Documentation Feedback	7-5 7-6

Index

iv

Index IN	Í –		l
----------	-----	--	---





vi



## Preface

## Preface

Topics include:

- Documentation on page 2
- Audience on page 3
- Document Conventions on page 3
- About Trend Micro on page 4



## **Documentation**

The documentation set for Deep Discovery Email Inspector includes the following:

**TABLE 1. Product Documentation** 

DOCUMENT	DESCRIPTION
Administrator's Guide	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.
Installation and Deployment Guide	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.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide contains information on event logging formats supported by Deep Discovery Email Inspector.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Email Inspector to your network and on performing the initial configuration.
Readme	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.
Online Help	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.

DOCUMENT	DESCRIPTION
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: <u>https://success.trendmicro.com</u>

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

http://docs.trendmicro.com/en-us/home.aspx/

## 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**

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options

CONVENTION	DESCRIPTION
Italics	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
Navigation > Path	The navigation path to reach a particular screen
	For example, <b>File</b> > <b>Save</b> means, click <b>File</b> and then click <b>Save</b> on the interface
Note	Configuration notes
<b>Г</b> р Тір	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

## **About Trend Micro**

Trend Micro, a global leader in cybersecurity, is passionate about making the world safe for exchanging digital information today and in the future. Artfully applying our XGen<sup>™</sup> security strategy, our innovative solutions for consumers, businesses, and governments deliver connected security for data centers, cloud workloads, networks, and endpoints.

Optimized for leading environments, including Amazon Web Services, Microsoft®, and VMware®, our layered solutions enable organizations to automate the protection of valuable information from today's threats. Our connected threat defense enables seamless sharing of threat intelligence and provides centralized visibility and investigation to make organizations their most resilient.

Trend Micro customers include 9 of the top 10 Fortune<sup>®</sup> Global 500 companies across automotive, banking, healthcare, telecommunications, and petroleum industries.

With over 6,500 employees in 50 countries and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. <u>https://www.trendmicro.com</u>



1-1

## **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

Feature	DESCRIPTION
QR code scanning	You can configure content filtering rules in Deep Discovery Email Inspector to perform actions on email messages with QR codes to protect against image- based QR code phishing attacks.
Trend Vision One integration	Deep Discovery Email Inspector integrates with Trend Vision One to enable collaborative security analytics in a hybrid environment.
	Important Before you can configure integration settings, apply the latest hotfix or patch.
Certificate management	You can manage certificates in Deep Discovery Email Inspector to enable secure console access and SMTP communication in Transport Layer Security (TLS) environments.
Email address modification	<ul> <li>Deep Discovery Email Inspector provides the email address modification feature that allows you to:</li> <li>Rewrite sender or recipient addresses in message envelops or message headers</li> <li>Rewrite domains in email addresses</li> </ul>

TABLE 1-1. New Features in Deep Discovery Email Inspector 5.1

1-2

FEATURE	DESCRIPTION
Enhanced TLS communications	TLS communications has been enhanced in Deep Discovery Email Inspector to support the following:
	• TLS 1.3
	<ul> <li>Secure connections for message transfer based on specified domains and IP addresses</li> </ul>
DANE for outbound messages	Deep Discovery Email Inspector supports DANE (DNS- based Authentication of Named Entities) to secure outbound messages by verifying SMTP server identity.
Enhanced policy settings	The policy management feature has been enhanced to provide the following settings:
	<ul> <li>Send a blind carbon copy (BCC) of detected messages to specified recipients</li> </ul>
	Change the recipients of detected messages
	Configure sender-recipient exceptions in policies
	<ul> <li>Configure address groups as policy objects</li> </ul>
	<ul> <li>Internal email spoofing prevention</li> </ul>
	<ul> <li>Apply message stamps based on policy rules</li> </ul>
Sender and recipient validation for Inbound messages	Deep Discovery Email Inspector provides the following security settings to enhance inbound message security:
	<ul> <li>Reject messages from unknown sender IP addresses or domains</li> </ul>
	<ul> <li>Reject messages to unknown recipients</li> </ul>
	<ul> <li>Match message header FROM address for sender filtering</li> </ul>
Enhanced Time-of-Click protection	The Time-of-Click protection feature has been enhanced to include the following:
	Customization of redirect pages for detected URLs
	<ul> <li>Syslog forwarding for detected URLs</li> </ul>

FEATURE	DESCRIPTION
Enhanced Virtual Analyzer	The Virtual Analyzer has been enhanced to include the following features:
	Open Document file type for sandbox analysis
	<ul> <li>Windows 10 20H1 image support</li> </ul>
Improved detection capability	Deep Discovery Email Inspector provides increased protection by improving its detection capabilities. This release supports the following:
	<ul> <li>ALG and EGG archive files for scanning</li> </ul>
	<ul> <li>Decryption of password-protected ALG and EGG archive files and Open Document files for scanning</li> </ul>
	<ul> <li>URL extraction from Open Document files for scanning</li> </ul>
	<ul> <li>DLP forensic data display on the Detections screens</li> </ul>
Enhanced approved and blocked senders lists	Configuration of the approved and blocked senders lists has been enhanced to include the following:
	<ul> <li>Sender list import and export</li> </ul>
	Wildcard support for email domain setting
Enhanced license management	The license management feature has been enhanced to support gateway-only license on Deep Discovery Email Inspector for gateway deployment.
New fiber network interface card (NIC) support	Deep Discovery Email Inspector supports additional data ports with 10Gbps fiber NIC installation on hardware models 7200, 7300, and 9200.
Deep Discovery Director 5.3 integration	Deep Discovery Email Inspector supports integration with Deep Discovery Director 5.3.
Deep Discovery Analyzer 7.0 integration	Deep Discovery Email Inspector supports integration with Deep Discovery Analyzer 7.0 to enable Linux ELF and shell script file submissions.

1-5

FEATURE	DESCRIPTION
Enhanced virtualized deployment	Deep Discovery Email Inspector supports virtual appliance installation on VMware ESXi 6.7 and 7.0.
Inline migration support	Deep Discovery Email Inspector provides users with the option of automatically migrating the settings from the following versions to 5.1:
	Deep Discovery Email Inspector 5.0
	Deep Discovery Email Inspector 3.6



2-1

## **Chapter 2**

## Deployment

Topics include:

- Deployment Overview on page 2-2
- Network Topology Considerations on page 2-3
- Recommended Network Environment on page 2-9
- Items to Prepare on page 2-10

## **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 2-3.

**2.** Review the system requirements.

See System Requirements on page 3-2.

3. Install Deep Discovery Email Inspector.

#### See the following:

- Installing Deep Discovery Email Inspector on a Hardware Appliance With an Optical Drive on page 3-10.
- Installing Deep Discovery Email Inspector on a Hardware Appliance Without an Optical Drive on page 3-11
- Installing Deep Discovery Email Inspector on a Virtual Appliance on page 3-14
- **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

### **MTA Mode**

2-4

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.



#### 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.



#### 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

4

2-8

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.

REQUIREMENT	DETAILS
Activation Code	Obtain from Trend Micro
Monitor and VGA cable	Connects to the VGA port of the appliance
USB keyboard	Connects to a USB port of the appliance
USB mouse	Connects to a USB port of the appliance
Ethernet cables	<ul> <li>Connect to the management and data ports</li> <li>Required: Management port (eth0) of the appliance to the management network</li> </ul>
	<ul> <li>Recommended: Data port (eth1, eth2, or eth3) connects to the custom network</li> </ul>
	<ul> <li>Optional: Unused data ports connect to the mail network for mail routing and monitoring</li> </ul>

### **Items to Prepare**

2-10

REQUIREMENT	DETAILS
Internet-enabled computer	Access to the management console from a computer with the following software installed:
	A supported web browser:
	<ul> <li>Microsoft Internet Explorer<sup>®</sup> 11</li> </ul>
	<ul> <li>Microsoft Edge<sup>™</sup></li> </ul>
	<ul> <li>Google Chrome<sup>™</sup> 66 or later</li> </ul>
	<ul> <li>Mozilla Firefox<sup>®</sup> 59 or later</li> </ul>
IP addresses	Required: One IPv4 address in the management network
	Recommended: One IPv4 address for the custom network
	<ul> <li>Optional: Two IPv4 addresses for the mail network and one IPv6 address for the management network</li> </ul>
Third party software licenses	Licenses for all third party software installed on sandbox images



3-1

## **Chapter 3**

## Installation

Topics include:

- System Requirements on page 3-2
- Integrated Trend Micro Products on page 3-5
- Ports Used by the Appliance on page 3-5
- Deep Discovery Email Inspector Installation on page 3-9
- Configuring Management Console Access on page 3-17
- The Management Console on page 3-19

## **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 the following:

- VMware ESXi 6.7, 7.0, or 8.0
- · Microsoft Hyper-V on Windows Server 2016, 2019, or 2022
- Nutanix AHV
- KVM (Kernel-based Virtual Machine)

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.
Messages Per Day	VIRTUAL CPUs*	Virtual Memory (GB)	Virtual Disk	VIRTUAL NICS**	DEEP Discovery Analyzer 1100 Appliance***
300K	3	10	500 GB	Refer to the following table	1 per 2 Deep Discovery Email Inspector virtual appliances
700K	6	16	1 TB	Refer to the following table	1 for each Deep Discovery Email Inspector virtual appliance

TABLE 3-1. Specifications for Virtual Applia
--

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

TABLE 3-2. Minimum virtual NIC requirements

OPERATION MODE	VIRTUAL NICS REQUIRED**	VIRTUAL NICS USED
BCC	1	ETH0 (data/management port)
МТА	1	ETH0 (data/management port)
SPAN/TAP	3	• ETH0 (management port)
		• ETH1 (reserved)
		• ETH2 (data port)



#### 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.

APPLICATION	REQUIREMENTS	DETAILS
SSH client	SSH protocol version 2	Set the Command Line Interface terminal window size to 80 columns and 24 rows.
Microsoft Edge™	Windows 10 or later	Use only a supported browser to
Mozilla Firefox™	Version 75 or later	Using the data port IP address you set during the initial configuration, specify the following URL:
Google Chrome™	Version 81 or later	
		https:// [Appliance_IP_Address]:443

**TABLE 3-3. System Access Requirements** 

### 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 4-25*.

## **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.

PRODUCT/ SERVICE	Version
Trend Vision One	
Deep Discovery Director - On- premises version	• 5.3
Deep Discovery Analyzer	• 7.0
	• 6.9
Apex Central	• 2019
Smart Protection Server	• 3.3
	• 3.2
TippingPoint Security Management	• 5.4
System (SMS)	• 5.3

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

## **Ports Used by the Appliance**

The following table shows the ports that are used with Deep Discovery Email Inspector and why they are used.

Port	PROTOCOL	FUNCTION	PURPOSE
22	ТСР	Listening	Endpoints connect to Deep Discovery Email Inspector through SSH.
25	ТСР	Listening	MTAs and mail servers connect to Deep Discovery Email Inspector through SMTP.
53	TCP/UDP	Outbound	<ul> <li>Deep Discovery Email Inspector uses this port for:</li> <li>DNS resolution</li> <li>Sender authentication (SPF, DKIM, DMARC) query</li> </ul>
80	ТСР	Listening and outbound	<ul> <li>Deep Discovery Email Inspector connects to other computers and integrated Trend Micro products and hosted services through this port.</li> <li>Connect to the Customer Licensing Portal to manage the product</li> </ul>
			Query Community File Reputation Services     Query Community Domain/IP Reputation Services
			<ul> <li>Query Web Reputation Services through the Smart Protection Network</li> </ul>
			<ul> <li>Upload virtual analyzer images to Deep Discovery Email Inspector using the image import tool</li> </ul>
			<ul> <li>Communicate with Trend Micro Apex Central if Deep Discovery Email Inspector is registered over HTTP</li> </ul>

TABLE 3-5. Ports used by Deep Discovery Email Inspector

Port	PROTOCOL	FUNCTION	Purpose
123	UDP	Outbound	Deep Discovery Email Inspector connects to the NTP server to synchronize time.
161	ТСР	Listening	Deep Discovery Email Inspector uses this port to listen for requests from SNMP managers.
162	ТСР	Outbound	Deep Discovery Email Inspector connects to SNMP mangers to send SNMP trap messages.

Port	PROTOCOL	FUNCTION	PURPOSE
443	ТСР	Listening and outbound	Deep Discovery Email Inspector uses this port to:
			Query Predictive Machine Learning engine
			Query Web Inspection Service
			<ul> <li>Access the management console with a computer through HTTPS</li> </ul>
			<ul> <li>Communicate with Trend Micro Apex Central</li> </ul>
			<ul> <li>Connect to the Smart Protection Network and query Web Reputation Services</li> </ul>
			<ul> <li>Connect to Trend Micro Threat Connect</li> </ul>
			<ul> <li>Send protected threat information to Smart Feedback</li> </ul>
			<ul> <li>Update components by connecting to the ActiveUpdate server</li> </ul>
			<ul> <li>Send product usage information to Trend Micro feedback servers</li> </ul>
			<ul> <li>Verify the safety of files through the Certified Safe Software Service</li> </ul>
			<ul> <li>Communicate with Deep Discovery Director - On-premises version</li> </ul>
			<ul> <li>Share threat intelligence information and exception list with other products</li> </ul>
4459	ТСР	Listening and outbound	Endpoints connect to the End-User Quarantine console on Deep Discovery Email Inspector through this port.

Port	PROTOCOL	FUNCTION	Purpose
5274	ТСР	Outbound	Deep Discovery Email Inspector uses this port as the default port to connect to the Smart Protection Server for web reputation services.
User-defined	N/A	Outbound	Deep Discovery Email Inspector uses specified ports to:
			<ul> <li>Send logs to syslog servers</li> </ul>
			<ul> <li>Share threat intelligence with integrated products/services</li> </ul>
			<ul> <li>Upload detection logs to SFTP servers</li> </ul>
			<ul> <li>Communicate with and Check Point Open Platform for Security (OPSEC)</li> </ul>
			<ul> <li>Connect to an LDAP server for third- party authentication and LDAP query</li> </ul>

## **Deep Discovery Email Inspector Installation**

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

Hardware appliance	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 <i>Configuring Management Console Access on page 3-17</i> .

Virtual appliance	Deep Discovery Email Inspector supports installation on the following:	
	• VMware ESXi 6.7, 7.0, or 8.0	
	Microsoft Hyper-V on Windows Server 2016, 2019, or 2022	
	Nutanix AHV	
	<ul> <li>KVM (Kernel-based Virtual Machine)</li> </ul>	
	For more information, see <i>Virtual Host Appliance Requirements on page 3-2</i> .	

## Installing Deep Discovery Email Inspector on a Hardware Appliance With an Optical Drive



#### 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**.

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

- 5. Click Accept.
- 6. Select the device to install Deep Discovery Email Inspector.
- 7. Click Continue.
- 8. At the warning message, click Yes to continue.

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

9. Click Next.

The **Summary** screen appears.

- 10. Click **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 3-17.

14. Open the management console.

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

For information about configuring Deep Discovery Email Inspector, see the Deep Discovery Email Inspector Administrator's Guide.

### Installing Deep Discovery Email Inspector on a Hardware Appliance Without an Optical Drive

For Deep Discovery Email Inspector appliances that do not include an optical drive, you can install Deep Discovery Email Inspector through the iDRAC (Integrated Dell Remote Access Controller) port.



#### WARNING!

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

#### Procedure

- Download the Deep Discovery Email Inspector installation ISO file from the License screen on the Business Success Portal at <u>https://success.trendmicro.com/dcx/s/license</u>.
- 2. Configure the iDRAC IP address. Do the following:
  - **a.** If the appliance is turned on, power off the appliance.
  - **b.** Connect the iDRAC port on the Deep Discovery Email Inspector appliance to a DHCP-enabled network.
  - **c.** Connect a monitor to the VGA port and attach a keyboard to a USB port on the appliance.
  - d. Power on or restart the appliance.

#### 👔 Note

The power button is found on the front panel of the appliance, behind the bezel.

- e. When the **power-on self-test (POST)** screen appears, press F2 to go to System Setup.
- **f.** Select **iDRAC Settings** > **Connectivity** > **Network**.
- **g.** In the **IPv4 Settings** section, disable **DHCP** and configure the required settings for the appliance to use a static IP address.
- **h.** Click **Apply** to save the changes.
- **3.** Log into the iDRAC interface. Do the following:
  - **a.** Open a web browser and go to the following address:

https://<idrac\_ip\_address>

The iDRAC login screen appears.

b. Specify the login credentials and click Log In.

The **Dashboard** appears.

- **4.** Turn off the appliance. On the **Dashboard**, select **Power Off System** from the **Graceful Shutdown** drop-down list.
- 5. Click Start Virtual Console.

A console screen appears.

- 6. Click Boot and select Virtual CD/DVD/ISO.
- Click Virtual Media and select Connect Virtual Media; then, click Connect Virtual Media.
- **8.** Under Map CD/DVD, click **Choose File** to select the Deep Discovery Email Inspector installation ISO file and click **Map Device**.

The system indicates the device is mapped successfully.

9. On the Dashboard, click Power On System.

Wait until the **Deep Discovery Email Inspector Appliance Installation** screen appears.

- 10. Select 1. Install Appliance and press ENTER.
  - When installing Deep Discovery Email Inspector via serial port, select **2. Install Appliance via Serial Port** and press ENTER.

The License Agreement screen appears.

- 11. Click Accept.
- 12. Select the device to install Deep Discovery Email Inspector.
- 13. Click Continue.
- 14. At the warning message, click **Yes** to continue.

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

15. Click Next.

The Summary screen appears.

- 16. Click **Continue** to begin the installation.
- 17. 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.

18. Configure network settings to access the management console.

For details, see Configuring Management Console Access on page 3-17.

19. Open the management console.

For details, see The Management Console on page 3-19.

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 With an Optical Drive 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 3-17.

8. Open the management console.

For details, see The Management Console on page 3-19.

For information about configuring Deep Discovery Email Inspector, see the *Deep Discovery Email Inspector Administrator's Guide*.

### **Setting Options for Virtual Appliance in ESXi**

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

#### Procedure

3-16

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.

- Mwara Toolo		
vmware roois		
Power Operations	Shut Down Guest	~
	Put Guest on Standby	~
	Power On / Resume VM	
	Restart Guest	~
Run VMware Tools Scripts	<ul> <li>✓ After powering on</li> <li>✓ After resuming</li> <li>✓ Before suspending</li> <li>✓ Before shutting down guest</li> </ul>	
Tools Upgrades	Check and upgrade VMware Tools before each power on	
Time	Synchronize guest time with host	
Power management	Expand for power management settings	

## **Configuring Management Console Access**

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.



- Host name
- IPv4 address
- Subnet mask
- IPv4 gateway
- Preferred IPv4 DNS
- Alternate IPv4 DNS
- IPv6 address
- 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.

## **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 *Requirements to Access Deep Discovery Email Inspector on page 3-4*.

For information about configuring required network settings before accessing the management console, see *Configuring Management Console Access on page 3-17*.

To log on, open a browser window and type the following URL:

https://<Appliance IP Address>



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

You can log on to the Deep Discovery Email Inspector management console using one of the following methods:

- Logging On Using Local Accounts on page 3-19
- Logging On With Single Sign-On on page 3-20

## **Logging On Using Local Accounts**

#### Procedure

1. On the **Log On** screen, type the logon credentials (user name and password) for the management console.

Use the default administrator logon credentials when logging on for the first time:

- User name: admin
- Password: ddei
- 2. Click Log On.
- **3.** If this is the first time you log on, change the account password before you can access the management console.

#### 👌 Note

For hardware model 7300, download and install Hotfix 1394 to display the correct hardware model information on the management console.

For more information, go to <u>https://success.trendmicro.com/dcx/s/</u> solution/000290725?language=en\_US.

## Logging On With Single Sign-On

If you configure the required settings for SAML integration on Deep Discovery Email Inspector, users can access the Deep Discovery Email Inspector management console using their existing identity provider credentials.

For information, see the Deep Discovery Email Inspector Administrator's Guide.

#### Procedure

- 1. On the Log On screen, select a service name from the drop-down list.
- 2. Click Single Sign-on (SSO).

The system automatically navigates to the logon page for your organization.

**3.** Follow the on-screen instructions and provide your account credentials to access the Deep Discovery Email Inspector management console.



# **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) 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



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

4-2

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



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.



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
<b></b>

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

Set the management port IP address	
Syntax:	
configure product management-port [ipv4   ipv6] <ip> <mask></mask></ip>	
View	Privileged
Parameters	ipv4: Configure IPv4 settings
	ipv6: Configure IPv6 settings
	<ip>: IP address for the interface</ip>
	<mask>: Network mask for the NIC</mask>
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	
Note Deep Discovery Email Inspector virtual appliances installed in Microsoft Hyper-V do not support SPAN/TAP 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.

#### Syntax:

configure network basic

View	Privileged
Parameters	None
Examples:	

\*\*\*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></dns2></dns1>		
View	Privileged	

Parameters	ipv4: Configure IPv4 settings
	ipv6: Configure IPv6 settings
	<dns1>: Primary DNS server</dns1>
	<dns2>: Secondary DNS server</dns2>
	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:

```
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

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:	
configure network hostname <hostname></hostname>	
View	Privileged
Parameters	<hostname>: The host name or fully qualified domain name (FQDN) for the Deep Discovery Email Inspector device</hostname>
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></mask></ip></interface>	
View	Privileged
Parameters	ipv4: Configure IPv4 settings
	ipv6: Configure IPv6 settings
	<interface>: NIC name</interface>
	<ip>: IP address for the interface</ip>
	<mask>: Network mask for the NIC</mask>
Example:	
To configure an NIC with the following values:	
• Interface: eth0	
• IPv4 address: 192.168.10.10	
• IPv4 subnet mask: 255.255.25.0	
configure network interface ipv4 eth0 192.168.10.10 255.255.255.0	

## configure network teaming reinit

#### TABLE 4-7. configure network teaming reinit

Disables network interface card (NIC) teaming and restores network card configuration		
Syntax:		
configure network teaming reinit		
View	Privileged	
Parameters	None	
Example:		

To disable NIC teaming:

configure network teaming reinit

## configure network route add

#### TABLE 4-8. configure network route add

Adds a new route entry	
Syntax:	
configure network	route add [ipv4   ipv6] <ip_prefixlen> <via> <dev></dev></via></ip_prefixlen>
View	Privileged
Parameters	ipv4: Configure IPv4 settings
	ipv6: Configure IPv6 settings
	<ip_prefixlen>: Destination network ID with format IP_Address/ Prefixlen</ip_prefixlen>
	<via>: IP address of the next hop</via>
	<dev>: Device name</dev>
Example:	
To add a new route en	try:
configure network route add ipv4 172.10.10.0/24 192.168.10.1 eth1	

## configure network route default

#### TABLE 4-9. configure network route default

syntax:		
View Privileged		

Parameter	ipv4: Configure IPv4 settings	
	ipv6: Configure IPv6 settings	
	<pre>sqateway&gt;: IP address of default gateway</pre>	
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

Deletes a route		
Syntax:		
configure network	<pre>c route del [ipv4   ipv6] <ip_prefixlen> <via> <dev></dev></via></ip_prefixlen></pre>	
View	Privileged	
Parameters	ipv4: Configure IPv4 settings	
	ipv6: Configure IPv6 settings	
	<b>&gt;ip_prefixlen&gt;</b> : Destination network ID with format IP_Address/ Prefixlen	
	<via>: IPv4 address of the next hop</via>	
	<dev>: Device name</dev>	
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		

#### TABLE 4-10. configure network route del

## configure network route del default/default ipv6

#### TABLE 4-11. configure network route del default/default ipv6

Deletes the default IPv6 gateway

#### 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 4-12. configure service nscd disable

Disables the name service cache daemon (nscd) at system startup.	
Syntax:	
configure service nscd disable	
View	Privileged
Parameters	None
Example:	
To disable the name service cache daemon at system startup:	
configure service nscd disable	

## configure service nscd enable

#### TABLE 4-13. configure service nscd enable

Enables the name service cache daemon (nscd) at system startup.	
Syntax:	
configure service nscd enable	
View	Privileged

Parameters	None
Example:	
To enable the name service cache daemon at system startup:	
configure service nscd enable	

## configure service ssh disable

#### TABLE 4-14. configure service ssh disable

Disables SSH on all network interface cards (NIC).		
Syntax:		
configure service ssh disable		
View	Privileged	
Parameters	None	
Examples:		
To disable SSH on all NICs:		
configure service ssh disable		

## configure service ssh enable

#### TABLE 4-15. configure service ssh enable

Enables SSH on one specific network interface card (NIC).		
Syntax:		
configure service ssh enable		
View	Privileged	
Parameters	None	
Examples:		

To enable SSH:

configure service ssh enable

## configure service ssh port

#### TABLE 4-16. configure service ssh port

Change SSH service port.	
Syntax:	
configure service ssh port <port></port>	
View	Privileged
Parameters	port: configure the SSH service port
	<port>: SSH service port number</port>
Example:	
To change the SSH service port to 56743: configure service ssh port 56743	

## configure service ntp

#### TABLE 4-17. configure service ntp

Synchronize the Deep Discovery Email Inspector system time with an NTP server.	
Syntax:	
configure service ntp [enable   disable   server-address <address>]</address>	
View	Privileged
Parameters	enable: Enable NTP
	disable: Disable NTP
	server-address: Configure the NTP server address
	<address>: Specify the FQDN or IP address of the NTP server</address>
Examples:	

#### To configure the NTP server address as 192.168.10.21:

configure service ntp server-address 192.168.10.21

#### To enable synchronization with the NTP server:

configure service ntp enable

## configure system date

#### TABLE 4-18. configure system date

Configures the time and date and saves the data in CMOS.	
Syntax:	
configure system date <date> <time></time></date>	
View	Privileged
Parameters	<date>: Set the date using the following format: yyyy-mm-dd</date>
	<time>: Set the time with the following format: hh:mm:ss</time>
Example:	
To set the date to August 12, 2010 and the time to 3:40 PM:	
configure system date 2010-08-12 15:40:00	

## configure system password enable

#### TABLE 4-19. configure system password enable

To change the password required to enter Privileged mode.		
Syntax:		
configure system password enable		
View	Privileged	
Parameters	None	
Examples:		

To change the password required to enter Privileged mode:

configure system password enable

## configure system timezone

#### TABLE 4-20. configure system timezone

Configures the time zone used by Deep Discovery Email Inspector.		
Syntax:		
configure system timezone <region> <city></city></region>		
View	Privileged	
Parameters	<region>: Region name</region>	
	<city>: City name</city>	
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 4-21. Time Zone Setting Examples

<b>REGION/COUNTRY</b>	Сіту
Africa	Cairo
	Harare
	Nairobi
America	Anchorage
	Bogota
	Buenos_Aires

REGION/COUNTRY	Сіту
	Caracas
	Chicago
	Chihuahua
	Denver
	Godthab
	Lima
	Los_Angeles
	Mexico_City
	New_York
	Noronha
	Phoenix
	Santiago
	St_Johns
	Tegucigalpa
Asia	Almaty
	Baghdad
	Baku
	Bangkok
	Calcutta
	Colombo
	Dhaka
	Hong_Kong
	Irkutsk

REGION/COUNTRY	Сітү
	Jerusalem
	Kabul
	Karachi
	Katmandu
	Krasnoyarsk
	Kuala_Lumpur
	Kuwait
	Magadan
	Manila
	Muscat
	Rangoon
	Seoul
	Shanghai
Asia (Continued)	Singapore
	Таіреі
	Tehran
	Токуо
	Yakutsk
Atlantic	Azores
Australia	Adelaide
	Brisbane
	Darwin
	Hobart

REGION/COUNTRY	Сіту
	Melbourne
	Perth
Europe	Amsterdam
	Athens
	Belgrade
	Berlin
	Brussels
	Bucharest
	Dublin
	Moscow
	Paris
Pacific	Auckland
	Fiji
	Guam
	Honolulu
	Kwajalein
	Midway
US	Alaska
	Arizona
	Central
	East-Indiana
	Eastern
	Hawaii
REGION/COUNTRY	Сіту
----------------	----------
	Mountain
	Pacific

# enable

### TABLE 4-22. enable

Enters privileged mode so privileged commands can be provided.		
Syntax:		
enable		
View	Normal	
Parameters	None	
Example:		
To enter privileged mode:		
enable		

# exit

#### TABLE 4-23. exit

Exits privileged mode.	
Exits the session for those not in privileged mode.	
Syntax:	
exit	
View	Normal
Parameters	None
Example:	

## To exit privileged mode or to exit the session when not in privileged mode:

exit

# help

### TABLE 4-24. help

Displays the CLI help information.		
Syntax:		
help		
View	Normal	
Parameters	None	
Example:		
To display the CLI help information:		
help		

# history

## TABLE 4-25. history

Displays the current session's command line history.	
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 4-26. logout

Logs out of the current CLI session.		
Syntax:		
logout		
View	Normal	
Parameters	None	
Example:		
To logout from the current session:		
logout		

# ping

# TABLE 4-27. ping

Pings a specified host.		
Syntax:		
ping [-c num_echos] [-i interval] <dest></dest>		
View	Normal	
Parameters	<b>[-c num_echos]</b> : Specifies the number of echo requests to be sent. Default value is 5.	
	[- <b>i interval</b> ]: Specifies the delay interval in seconds between each packet. Default value is 1 second.	
	<dest>: Specifies the destination host name or IP address</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 4-28. ping6

Pings a specified IPv6 host through interface eth0.	
Syntax:	
ping6 [-c num_echos] [-i interval] <dest></dest>	
View	Normal
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</dest>
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 4-29. start task postfix drop

Deletes a specified message or all messages in the email message queue.	
Syntax:	
<pre>start task postfix drop { <mail_id>   all }</mail_id></pre>	
View	Privileged

Parameters	<mail_id>: Specifies the message ID in the postfix queue to delete</mail_id>	
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 4-30. start task postfix flush

Attempts to deliver all queued email messages.		
Syntax:		
start task postfix flush		
View	Privileged	
Parameters	None	
Example:		
To deliver all queued email messages:		
start task postfix flush		

# start task postfix queue

### TABLE 4-31. start task postfix queue

Displays all email messages queued in Postfix.	
Syntax:	
start task postfix queue	
View	Privileged
Parameters	None

### Example:

### To display all Postfix queued email messages:

start task postfix queue

# start service nscd

#### TABLE 4-32. start service nscd

Starts the name service cache daemon (nscd).		
Syntax:		
start service nscd		
View	Privileged	
Parameters	None	
Example:		
To start the name service cache daemon:		
start service nscd		

# start service postfix

### TABLE 4-33. start service postfix

Starts the Postfix mail system	
Syntax:	
start service postfix	
View	Privileged
Parameters	None
Example:	
To start the Postfix mail system:	
start service postfix	

# start service product

#### TABLE 4-34. start service product

Starts the Product service system.	
Syntax:	
start service product	
View	Privileged
Parameters	None
Example:	
To start the Product service system:	
start service product	

# start service ssh

### TABLE 4-35. start service ssh

Starts the ssh service system.	
Syntax:	
start service ssh	
View	Privileged
Parameters	None
Example:	
To start the ssh service system:	
start ssh service	

### stop process core

### TABLE 4-36. stop process core

Stops a running process and generates a core file.

Syntax:	
stop process core <pid></pid>	
View	Privileged
Parameters	<pid>: The process ID</pid>
Example:	
To stop a process with ID 33:	
stop process core 33	

# stop service nscd

#### TABLE 4-37. stop service nscd

Stops the name service cache daemon (nscd).	
Syntax:	
stop service nscd	
View	Privileged
Parameters	None
Example:	
To stop the name service cache daemon:	
stop service nscd	

# stop service postfix

### TABLE 4-38. stop service postfix

Stops the Postfix mail system.	
Syntax:	
stop service postfix	
View Privileged	

Parameters	None
Example:	
To stop the Postfix mail system:	
stop service postfix	

# stop service product

### TABLE 4-39. stop service product

Stops the Product service system.		
Syntax:		
stop service product		
View	Privileged	
Parameters	None	
Example:		
To stop the Product service system:		
stop service product		

# stop service ssh

## TABLE 4-40. stop service ssh

Stops the ssh service system.	
Syntax:	
stop service ssh	
View	Privileged
Parameters	None
Example:	

To stop the ssh service system:

stop ssh service

# reboot

### TABLE 4-41. reboot

Reboots the Deep Discovery Email Inspector appliance immediately or after a specified delay.		
Syntax:		
reboot [time]		
View	Privileged	
Parameters	<b>[time]</b> : Specifies the delay, in minutes, to reboot the Deep Discovery Email Inspector appliance	
Examples:		
To reboot the Deep Discovery Email Inspector appliance immediately:		
reboot		
To reboot the Deep Discovery Email Inspector appliance after 5 minutes:		
reboot 5		

# resolve

#### TABLE 4-42. resolve

Resolves an IPv4 address from a host name or resolves a host name from an IPv4 address.	
Syntax:	
resolve <dest></dest>	
View	Privileged
Parameter	<dest>: Specifies the IPv4 address or host name to resolve</dest>
Examples:	

To resolve the host name from IP address 192.168.10.1:

resolve 192.168.10.1

To resolve the IP address from host name parent.host.com:

resolve parent.host.com

## show storage statistic

#### TABLE 4-43. show storage statistic

Displays the file system disk space usage.		
Syntax:		
show storage statistic [partition]		
View	Normal	
Parameters	[partition]: Specify a partition. This is optional.	
Example:		
To display the file system disk space usage of the Deep Discovery Email Inspector appliance:		
show storage statistic		

### show network

#### TABLE 4-44. show network

Displays various Deep Discovery Email Inspector network configurations.

#### Syntax:

```
show network [arp <address> | connections | dns | dns ipv6| hostname
| interface | route | route ipv4 | route default ipv4 | route default
ipv6]
```

View Normal

Parametersarp: Displays the value returned by the Address Resolution (ARP) for the given address.			
	<b><address></address></b> : FQDN or IP address that will be resolved with the Address Resolution Protocol (ARP).		
	<b>connections</b> : Displays the current network connections of the Deep Discovery Email Inspector appliance.		
<b>dns</b> : Displays the DNS IP address of the Deep Discovery Email In appliance.			
<b>dns ipv6</b> : Displays system DNS configuration for IPv6.			
	<b>hostname</b> : Displays the host name of the Deep Discovery Email Inspector appliance.		
	<b>interface</b> : Displays the network interface card (NIC) status and configuration.		
	route: Displays IP address route table.		
	route ipv4: Displays system IPv4 route table.		
	route default ipv4: Displays default IPv4 route table.		
	route default ipv6: Display default IPv6 route table.		
Examples:			
To display the ARP inf	ormation 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	S configuration for IPv6:		
show network dns ipv6			
To display the host na	me 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 4-45. show kernel

Displays the OS kernel information of the Deep Discovery Email Inspector appliance.

#### Syntax:

show kernel {messages | modules | parameters | iostat}

View	Normal
Parameters	messages: Displays kernel messages.
	modules: Displays kernel modules.
	parameters: Displays kernel parameters.
	<b>iostat</b> : Displays CPU statistics and I/O statistics for devices and partitions.
Francia a.	

#### 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 4-46. show service

Displays the Deep Discovery Email Inspector service status.				
Syntax:				
show service [ntp	<pre><enabled server-address=""  ="">   ssh   nscd]</enabled></pre>			
View	Normal			
Parameters	<b>nscd</b> : Displays the status of the name service cache daemon.			
	ntp enabled: Displays the system NTP service status.			
	<b>ntp server-address</b> : Displays the system NTP service server address.			
	<b>ssh</b> : Displays the status of SSH.			
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 4-47. show memory

Displays the system memory information.		
Syntax:		
show memory [vm   statistic]		
View	Normal	
Parameters	<b>vm</b> : Displays virtual memory statistics	
	statistic: Displays system memory statistics	
Examples:		
To display the virtual memory statistics:		
show memory vm		
To display the system memory statistics:		
show memory statistic		

# show process

## TABLE 4-48. showprocess

Displays the status of the processes that are currently running.		
Syntax:		
show process [top   stack   itrace   trace] [pid]		
View	Normal	
Parameters	<b>top</b> : Displays the status of the processes that are currently running and system related processes	
	<b>stack</b> : Print a stack trace of a running process	
	itrace: Trace the library call	
	trace: Trace system calls and signals	
<b>pid</b> : 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 4-49. show product-info

Displays the product information.				
Syntax:				
show product-info [management-port   operation-mode   service-status   version				
View	Normal			
Parameters	<b>management-port</b> : Displays the management port's IP address and subnet mask			
	<b>operation-mode</b> : Displays the operation mode of Deep Discovery Email Inspector			
	service-status: Displays the status of services			
	<b>version</b> : Displays the product version			
Examples:				

To display the management port's IP address and mask: show product-info managementport

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 4-50. show system

Displays various system settings.

#### Syntax:

```
show system [date | timezone [continent | city | country]| uptime |
version]
```

View	Normal			
Parameters	date: Displays the current time and date.			
	<b>timezone</b> : Displays the timezone settings. You can optionally specify the timezone information to view:			
	<ul> <li>continent: Displays the system continent</li> </ul>			
	• <b>city</b> : Displays the system city			
	country: Displays the system country			
	<b>uptime</b> : Displays how long the Deep Discovery Email Inspector appliance has been running.			
	<b>version</b> : Displays version number for the Deep Discovery Email Inspector appliance.			
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 4-51. shutdown

Specifies shutting down the Deep Discovery Email Inspector appliance immediately or after a specified delay.

Syntax:

shutdown [time]

View	Privileged
Parameters	<b>[time]</b> : Shuts down the Deep Discovery Email Inspector appliance after a specified delay in minutes.
Examples:	
To shut down the Dee	p Discovery Email Inspector appliance immediately:
shutdown	

4-37

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

shutdown 5

# traceroute

#### **TABLE 4-52. traceroute**

Displays the tracking route to a specified destination.			
Syntax:			
traceroute [-h hops] <dest></dest>			
View	Normal		
Parameters	<b>[-h hops]</b> : Specifies the maximum number of hops to the destination. The minimum number is 6.		
	<dest>: Specifies the remote system to trace</dest>		
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			



5-1

# **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

System Update	DESCRIPTION			
Hotfix	A hotfix is a workaround or solution to a single customer-reported issue. Hotfixes are issue-specific, and are not released to all customers.			
	Note A new hotfix may include previous hotfixes until Trend Micro releases a patch.			
Security patch	A security patch focuses on security issues suitable for deployment to all customers. Non-Windows patches commonly include a setup script.			
Patch	A patch is a group of hotfixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis.			

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:

http://downloadcenter.trendmicro.com/

# **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 <u>http://downloadcenter.trendmicro.com</u>.

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 <u>http://downloadcenter.trendmicro.com</u>.

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 5.0 or 3.6 to Deep Discovery Email Inspector 5.1 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.
- 6. Browse for the firmware update package.
- 7. Click Install.

# 🔵 Тір

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 5.1 with a configuration file backed up from a server running version 3.2 or earlier versions.

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

# A 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.

LICENSE ACTIVATION	Advanced Threat Protection + Gateway Module	GATEWAY MODULE Only	Advanced Threat Protection Only
Advanced Threat Protection + Gateway Module	Compatible	Compatible	Compatible
GATEWAY MODULE Only	Not compatible	Compatible	Not compatible
Advanced Threat Protection Only	Not compatible	Not compatible	Compatible

#### TABLE 5-2. License compatibility



6-1

# **Chapter 6**

# **Creating a New Virtual Appliance**

Learn how to create a virtual appliance in the supported virtual environments in the following sections:

- Creating a VMWare ESXi Virtual Appliance on page 6-2
- Creating a Virtual Machine in Microsoft Hyper-V on page 6-9
- Creating a Virtual Machine using KVM on page 6-31
- Creating a Virtual Machine on Nutanix AHV on page 6-38

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 6-5

# **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**.

<b>vm</b> vv	are	
User name		<b>vm</b> ware <sup>,</sup> Esxi <sup>,,</sup>
	Log in	

**2.** Click **Networking** and then click the **Virtual switches** tab. Observe the initial state.

mware' ESXi' Q Seed								
T Navigator	A Metworki	ng						
+ 🛙 Host	Port groups Virtual switches	Physical NICs VMkernel NICs TCP/IP stacks	Firewall rules					
Gringe	> ∰ Writaul Machines ▲ Add standard vitual switch III, Add uplinix							
📲 👷 Networking	Name	<ul> <li>Port groups</li> </ul>	v Uplinks	~ Type	~			
> 🔜 vmk0	an vowitch0	3	1	Standard vSwitch				
tap port group	New switch	1	2	Standard vSwitch				
More networks	iestswitch	0	1	Standard vSwitch				
					3 items 🦼			

- **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.

Add standard virtual switch - Ma	nagement Network	
📇 Add uplink		
vSwitch Name	Management Network	
MTU	1500	
Uplink 1	vmnic3 - Down	$\otimes$
Link discovery	Click to expand	
✓ Security		
Promiscuous mode	O Accept      Reject	
MAC address changes	O Accept      Reject	
Forged transmits	Accept   Reject	
	Add	incel

c. Click Add.

vmware' esxi'					• I Help	<ul> <li>I Q Search</li> </ul>
T Navigator	Anteresting					
> 🛙 Hast	Port groups Virtual switches Physica	I NICs VMkemel NICs TO	PAP stacks Firewall rules			
Griver Machines     Storage	🏡 Add standard virtual switch 🛛 🚊 Add uplink	🥖 Edit settings   🙋 Refresh	- Actions			Q Search
- 🔮 Networking 🔤 📑	Name	<ul> <li>Port groups</li> </ul>	~	Uplinks	Type	~
> 📷 vmk0	📾 v8wtxh0	3		1	Standard vSwitch	
tap port group	New switch	1		2	Standard vSwitch	
More networks	in testswitch	0		1	Standard vSwitch	
	Im Nanagement Network	a		0	Standard vOwitch	
						4 items

**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.

没 Add port group - Management Port G	roup
Name	Management Port Group
VLAN ID	1000
Virtual switch	Management Network
✓ Security	
Promiscuous mode	○ Accept ○ Reject ● Inherit from vSwitch
MAC address changes	Accept Reject Inherit from vSwitch
Forged transmits	○ Accept ○ Reject ● Inherit from vSwitch
	Add Cancel

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



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

fanagement i	Port Group	Actions	
	Management Pol Accessible: Virtual machines: Virtual switch: VLAN ID: Active ports:	t Group	Yes 0 Management Network 1000 0
VSwitch top	nology ment Port Group 1000		Physical adapters

# **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.

ն New virtual machine			
<ul> <li>Select creation type</li> <li>Select a name and guest OS</li> <li>Select storage</li> </ul>	Select creation type How would you like to create a Virtual Machine?		
4 Customize settings 5 Ready to complete	Create a new virtual machine Deploy a virtual machine from an OVF or OVA file Register an existing virtual machine		This option guides you through creating a new virtual machine. You will be able to customize processors. memory, newtork connections, and storage You will need to install a guest operating system after creation.
<b>vm</b> ware		~	
			Back Next Finish Cancel

- 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 7.0 U1 virtual machine.
  - c. For Guest OS family, select Linux.

6-6

d. For Guest OS version, select CentOS 7 (64-bit).

1 Select creation type	Select a name and gues	st OS	
2 Select a name and guest OS 3 Select storage	Specify a unique name and OS		
4 Customize settings	Name		
5 Ready to complete	New Virtual machine		
	Virtual machine names can contain u	up to 80 characters and they must be unique within each ES	SXi instance.
	Identifying the guest operating system installation.	m here allows the wizard to provide the appropriate defaults	for the operating syste
	Compatibility	ESXi 7.0 U1 virtual machine	$\sim$
	Guest OS family	Linux	$\checkmark$
	Guest OS version	100000000 <sup>22</sup> (0011000)	~

- 4. Click Next.
- 5. On the **Select storage screen**, select the destination storage where the virtual machine resides and click **Next**.

🎦 New virtual machine - New Virtual machine (ESXi 7.0 U1 virtual machine)										
<ul> <li>✓ 1 Select creation type</li> <li>✓ 2 Select a name and guest OS</li> <li>✓ 3 Select storage</li> <li>✓ 4 Customize settings</li> <li>✓ 5 Ready to complete</li> </ul>	Select storage Select the storage type and datastore Standard Persistent Memory Select a datastore for the virtual machine	's co	nfiguration files	and all (	of its' v	irtual disk:	3.			
	Name	~	Capacity ~	Free	~	Туре	~	Thin pro $\sim$	Access	~
	datastore1		6.42 TB	5.9 TB		VMFS6		Supported	Single	
									1 iten	ns
<b>vm</b> ware										
					Bac		Next	Finish	Can	icel

- 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.
      - 1. Set the VMware ESXi server **VM Network** as the Deep Discovery Email Inspector Management Network (NIC 1).
      - 2. Set the **Data port group** as the Deep Discovery Email Inspector Data Network (NIC 2).
      - 3. For Adapter Type, select VMXNET 3.
- 7. Click Next.

<ul> <li>1 Select creation type</li> <li>2 Select a name and guest OS</li> <li>3 Select storage</li> </ul>	Ready to complete Review your settings selection before	re finishing the wizard
4 Customize settings	Name	New Virtual machine
5 Ready to complete	Datastore	datastore1
	Guest OS name	CentOS 7 (64-bit)
	Compatibility	ESXi 7.0 U1 virtual machine
	vCPUs	3
	Memory	10 GB
	Network adapters	3
	Network adapter 1 network	test port group
	Network adapter 1 type	VMXNET 3
	Network adapter 2 network	test port group
	Network adapter 2 type	VMXNET 3
	Network adapter 3 network	tapping port group
	Network adapter 3 type	VMXNET 3
	IDE controller 0	IDE 0
<b>vm</b> ware <sup>®</sup>	IDE controller 1	IDE 1
	SCSI controller 0	VMware Paravirtual

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.

∎∎н	lyper-V Manager		- 🗆 X
File	Action View Help		
🦛 =	New >		
H	Import Virtual Machine		Actions
	Hyper-V Settings	3	WIN-2PFLUH4Q1Q
	Virtual Switch Manager	State CPU Usage Assigned Memory Uptime Status	New 🕨
	Virtual SAN Manager	No virtual machines were found on this server.	🛝 Import Virtual Machine
	Edit Disk		Hyper-V Settings
	Inspect Disk		Strual Switch Manager
	Ston Service		June 1 Virtual SAN Manager
	Remove Server		Edit Disk
	Refresh		Inspect Disk
	Help	$\odot$	Stop Service
1		No vitual machine selected	× Remove Server
			🖏 Refresh
			View
			Help
			- ·
	Details		1
		No item selected	
		No Kell Speciel.	1
Display	us the Virtual Switch Manager user interfac	79.	1

**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.

Virtual Switches	🛃 Virtual Switch Properties ————————————————————————————————————				
New virtual network switch	Manag				
Management Switch Intel(P) 82576 Gigabit Dual P	Name:				
Global Network Settings	[Management Switch]				
MAC Address Range	Notes:				
	Connection type				
	What do you want to connect this virtual switch to?				
	External network:				
	Intel(R) 82576 Gigabit Dual Port Network Connection $\sim$				
	Allow management operating system to share this network adapter				
	Enable single-root I/O virtualization (SR-IOV)				
	O Private network				
	VIANID				
	Enable virtual LAN identification for management operating system				
	The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.				
	virtual switch with SR-IOV enabled cannot be converted to an internal or private switch.				

g. Click Apply.

6-12

The Apply Networking Changes confirmation window appears.

Virtual Switches     New virtual network switch     La Management Switch     Intel(R) 82576 Gigal     Global Network Settings	Virtual Switch Pr Name: Management Switch Notes:	operties ———			
🦉 MAC Address Kange	Apply Netw Apply Netw Col Thi the opp ove mu cor	working Changes X ending changes may disrupt network onnectivity his computer may lose its network connection while te changes are applied. This may affect any network perations in progress. These changes also may verwrite some static changes. If that happens, you ust reapply the static changes to restore network			ction ~
	Please	don't ask me again The VLAN identifies system will use for setting does not a 2 SR-IOV can only virtual switch switch	Yes r specifies the viri- r all network comm ffect virtual mach y be configured with SR-IOV enable	No ror management ual LAN that the unications throu ine networking, then the virtual s d cannot be con	c operating system = management operating ugh this network adapter. This Remove witch is created. An external verted to an internal or private

- 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.

- 1. 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.

File A	er-V Manager Action View Help			- 🗆 X
<b>(= =</b>	New >	Virtual Machine		
H	Import Virtual Machine	Hard Disk		Actions
	Hyper-V Settings	Floppy Disk		WIN-2PFLIJH4Q1Q
	Virtual Switch Manager	I Switch Manager State CPU Usage Assigned Memory Uptime Status		New
	Virtual SAN Manager	No virtual machine	es were found on this server.	🕵 Import Virtual Machine
	Edit Disk			👔 Hyper-V Settings
	Inspect Disk			🟭 Virtual Switch Manager
	Stop Service			🔒 Virtual SAN Manager
	Remove Server			🛃 Edit Disk
	Refresh		🔄 Inspect Disk	
	Help		۲	<ul> <li>Stop Service</li> </ul>
		No virtua	🗙 Remove Server	
			🖏 Refresh	
				View
				👔 Help
	Details			
		No	item selected.	
Disularia	the New York of Marchine Mercud			
probleta a	are new oncoarmachine wizdru.			

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.

New Virtual Machine Wiz Specify Name	ard ne and Location	×
Before You Begin Specify Name and Location Specify Generation	Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you eas identify this virtual machine, such as the name of the guest operating system or workload.	ily
Assign Memory Configure Networking Connect Virtual Hard Disk	Name:         Deep Discovery Email Inspector           You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.	
Installation Options Summary	Store the virtual machine in a different location Location: C:ProgramData/Wicrosoft/Windows/Hyper-V Browse.	
	▲ If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.	
	< Previous Next > Einish Cancel	

d. Click Next.

The **Specify Generation** screen appears.

e. Select Generation 1.

🖳 New Virtual Machine Wiza	ard X
🚬 Specify Gene	eration
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	<ul> <li>Choose the generation of this virtual machine.</li> <li> <ul> <li>Generation 1</li> <li>This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual machine generation support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.</li> <li>Once a virtual machine has been created, you cannot change its generation.</li> </ul> </li> <li>More about virtual machine generation support</li> </ul>
	< Previous Next > Finish Cancel

f. Click Next.

The Assign Memory screen appears.

g. For Startup memory, assign at least 10240 MB (10 GB).

New Virtual Machine Wiz Assign Men	ard ×
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system. Startup memory: 10244 MB Use Dynamic Memory for this virtual machine. When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.
	< Previous Next > Finish Cancel

h. Click Next.

The **Configure Networking** screen appears.

i. For Connection, select Management Switch.

👱 New Virtual Machine Wizar	d X
🛀 Configure Ne	etworking
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. Connection: Management Switch
	< Previous Next > Finish Cancel

j. Click Next.

6-18

The Connect Virtual Hard Disk screen appears.

k. Select Attach a virtual hard disk later.

Before You Begin Specify Name and Location Specify Generation	A virtual machine storage now or o O greate a virt	requires storage so that you can install an operating system. You configure it later by modifying the virtual machine's properties. Wal hard disk	can specify the
Assign Memory Configure Networking	Name:	Daeo Discovery Email Inspector yody	
Connect Virtual Hard Disk	Location:	C: Users \Public \Documents \Hyper-V\Virtual Hard Disks \	Browse
Summary	Size:	127 GB (Maximum: 64 TB)	
	Use an exist	ng virtual hard disk on to attach an existing virtual hard disk, either VHD or VHDX form	at.
	Location:	C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\	Browse
	<u>A</u> ttach a virt	ual hard disk later	

I. 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**.

lew	Virtual Machine	-							
mport Virtual Machine	Hard Disk								Actions
lyper-V Settings	Floppy Disk								WIN-IR67DEDSIF
firtual Switch Manager firtual SAN Manager	3WIN2016	State Off	CPU Usage	Assigned Memory	Uptime	Status	Configurati 8.0	Replication Health Not Applicable	New Pt. Import Virtual Machine
dit Disk nspect Disk	5 Liscovery Email Insp.	Ue .					6.0	Not Applicable	Hyper-V Settings
itop Service									Virtual SAN Manager
sernove server lefresh									Z Edit Disk
Help									Stop Service
									× Remove Server
									Refresh
									View
								(d) Starts (d) James	
	<							,	
	Checkpoints							۲	
	Details								
				,	io item selected.				

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

**b.** Click **Next**.

The **Choose Disk Format** screen appears.

c. Select VHDX.

🏝 New Virtual Hard Disk Wiz	ard X
🏝 Choose Disk	Format
Before You Begin Choose Disk Format Choose Disk Type Specify Name and Location Configure Disk Summary	<ul> <li>What format do you want to use for the virtual hard disk?</li> <li>VHD Supports virtual hard disks up to 2,040 GB in size.</li> <li>V VHDX This format supports virtual disks up to 64 TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012.</li> <li>VHD Set This format is for shared virtual hard disks only, and enables backup of virtual machine groups using shared virtual hard disks. This format is not supported in operating systems earlier than Windows 10.</li> </ul>
	< Previous Next > Finish Cancel

d. Click Next.

The **Choose Disk Type** screen appears.

e. Select Fixed size.

🏝 New Virtual Hard Disk Wiz	card X
🚢 Choose Disk	түре
Before You Begin Choose Disk Format Choose Disk Type Specify Name and Location Configure Disk Summary	<ul> <li>What type of virtual hard disk do you want to create?</li> <li>Fixed size This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added. Dynamically expanding This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual hard disk file that is created is small initially and changes as data is added. Differencing This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easly. All children must have the same virtual hard disk format as the parent (VHD or VHDX).</li></ul>
	< Previous Next > Finish Cancel

f. Click Next.

6-22

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

g. For Name, type Deep Discovery Email Inspector.vhdx.

🏝 New Virtual Hard Disk W	izard	×
💄 Specify Nar	ne and Location	
Before You Begin Choose Disk Format Choose Disk Type	Specify the name and location of the virtual hard disk file. Name: Deep Discovery Email Inspector.vhdx	]
Specify Name and Location	Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\	Browse
Configure Disk		
Summary		
	< Previous Next > Einish	Cancel

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.

Before You Begin Choose Disk Format Choose Disk Type Specify Name and Location	You can create a blank virtual hard disk or copy the conten © Create a new blank virtual hard disk gize: 500 GB (Maximum: 64 TB) O Copy the contents of the specified physical disk:	ts of an existing physical disk.
Summary	Physical Hard Disk [], PHYSICALDRIVE0 Copy the contents of the specified <u>virtual hard disk </u>	Size 3725 G8

k. Click Next.

The Completing the New Virtual Hard Disk Wizard screen appears.

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



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

View State CHU Usage Assigned Menory Uptime States Configuration State Of Usage Assigned Menory Uptime States Configuration State States S	Replication Health Not Applicable Not Applicable	WIN-IR67QEQSIF New Import Virtual Machine
The SCRENDES of United Analysis Memory Opens 2004 Comparison Compared Analysis Com Analysis Compared Analysis Compared A	Kepincation Health Not Applicable Not Applicable	New https://www.internet/
Company and sparse of	Not Applicable	C Import Virtual Machine
		E. Human V Sattians
		and the second s
		Virtual Switch Manager
		Virtual SAN Manager
		d Edit Disk.
		D Inspect Disk.
		Son Senire
		¥ Remove Server
		D Refush
		View
		10 Hala
		E nep
		Deep Discovery Email Inspect
		Connect
		Settings
		Start
		B Checkpoint
		P Move
		Export
		🛒 Rename
< c	>	Belete
Checkpoints	۲	1 Enable Replication
		Help
Deep Discovery Email Inspector		
Replication Hode: Not evabled Primary Server:		
Replication State: Not enabled Replica Server:		
Replication Health: Not Applicable Last synchronized at: Not Applicable		

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.

Deep Discovery Email Inspector	✓ ◀ ► ♡	
t Hardware	Processor	
Add Hardware		
BIOS Boot from CD	You can modify the number of virtual proce the physical computer. You can also modify	essors based on the number of processors o y other resource control settings.
Security Key Storage Drive disabled	Number of virtual processors:	β.♥
Memory	Resource control	
12288 MB	You can use resource controls to balance	e resources among virtual machines.
Processor 3 Virtual processors	Virtual machine reserve (percentage):	0
B IDE Controller 0	Percent of total system resources:	0
Hard Drive Deep Discovery Email Insp	Virtual machine limit (percentage):	100
E IDE Controller 1	Percent of total system recourses:	6
DVD Drive     None	Percent of total system resources.	
SCSI Controller	Relative weight:	100
Network Adapter Management Switch	This virtual machine is configured with	the following:
Network Adapter TAPPING	Sockets: 3 NIMA podes per socket: 1	
COM 1	Virtual processors per NUMA node: 1 Memory per NUMA node: 62846 MB	
COM 2		
None		
Diskette Drive None		
Management		
Name Deep Discovery Email Inspector		
Some services		
Checkpoints Production		

- 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.

	~	લ ⊩ છ				
Hardware	^	- Hard Drive -				
Add Hardware     BIOS     Boot from CD		You can change how operating system is i virtual machine from	this virtual hard nstalled on this o starting.	l disk is attache disk, changing t	ed to the virtual ma the attachment mig	schine. If an ght prevent the
Security		Controller:		Locat	ion:	
Key Storage Drive disabled		IDE Controller 0		~ 0 (in	use)	
8192 MB		Media				
Processor 4 Virtual processors		You can compact, by editing the ass	convert, expan ociated file. Spe	d, merge, reco cify the full pat	nnect or shrink a v h to the file.	rirtual hard disk
IDE Controller 0			sk:			
Hard Drive Deep Discovery Email I	-	C:\Users\Pub	lic\Documents\H	yper-V\Virtual	hard disks\Deep Di	iscovery Email In:
IDE Controller 1			New	Edit	Inspect	Browse
DVD Drive None		O Physical hard	disk:			-
SCSI Controller						
0						
Network Adapter Management Switch		16 the ch	unical based diels :	and the second terms	a is not listed mak	o cura that the
Network Adapter Management Switch COM 1		If the ph disk is of	ysical hard disk fline. Use Disk M	you want to us anagement on	e is not listed, mak the physical comp	e sure that the uter to manage
<ul> <li>Network Adapter Management Switch</li> <li>COM 1 None</li> </ul>		If the ph disk is of physical	ysical hard disk fline. Use Disk M hard disks.	you want to us anagement on	e is not listed, mak the physical comp	e sure that the uter to manage
Network Adapter Management Switch     OM 1 None     COM 2 None		If the ph disk is of physical To remove the virtue delete the associate	ysical hard disk fline. Use Disk M hard disks. al hard disk, click d file.	you want to us anagement on Remove. This	e is not listed, mak the physical comp disconnects the de	sk but does not
Network Adapter Management Switch OOM 1 None COM 2 None Diskette Drive None		If the ph disk is of physical To remove the virtua delete the associated	ysical hard disk ; fline. Use Disk M hard disks. al hard disk, click d file.	you want to us anagement on Remove. This	e is not listed, mak the physical comp disconnects the de	e sure that the uter to manage sk but does not Remove
Network Adapter Management Switch OOM 1 None OOM 2 None Diskette Drive None Management		If the ph disk is of physical To remove the virtue delete the associated	ysical hard disk ; fline. Use Disk M hard disks. al hard disk, click d file.	you want to us anagement on Remove. This	e is not listed, mak the physical comp disconnects the de	e sure that the uter to manage sk but does not <u>R</u> emove
Network Adapter Management Switch COM 1 None COM 2 None Diskette Drive None Management Name Despectory Email Inspector	_	<ul> <li>If the ph disk is of physical</li> <li>To remove the virtue delete the associated</li> </ul>	ysical hard disk ; fine. Use Disk M hard disks. Il hard disk, dick d file.	you want to us anagement on Remove. This	e is not listed, mak the physical comp disconnects the di	e sure that the uter to manage sk but does not <u>R</u> emove
	_	If the ph disk is of physical     To remove the virtue delete the associated	ysical hard disk y filne. Use Disk M hard disks. Il hard disk, dick d file.	you want to us anagement on Remove. This	e is not listed, mak the physical comp disconnects the di	sk but does not
Network Adapter Management Switch COM 1 None COM 2 None Descette Drive None Management Name Deep Discovery Email Inspector Integration Services Some services offered Checkpoints Production	,	If the ph disk is of physical     To remove the virtue delete the associated	ysical hard disk fine. Use Disk M hard disks. I hard disk, dick d file.	you want to us anagement on Remove. This	e is not listed, mak the physical comp disconnects the di	ke sure that the uter to manage sk but does not Remove

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.

1. For the devices you want to add, select Network Adapter.

Deep Discovery Email Inspector	$\sim$	∢ ▶ 0		
A Hardware	^	Add Hardware		
Add Hardware				
BIOS		You can use this setting to add devices to your virtual machine.		
Boot from CD		Select the devices you want to add and click the Add button.		
Security		SCSI Controller		-
Key Storage Drive disabled		Network Adapter		
WW Memory		RemoteFX 3D Video Adapter		
8192 MB		Legacy Network Adapter		
Virtual processors		Fibre Channel Adapter		
= IDE Controller 0		Remoter% 30 Mideo Adaptor	Add	1
+ - Hard Drive		Leoney Network Adapter	AUG	
Deep Discovery Email Insp.		Virtual machines are created with one network adapter. You can	add additional net	two
IDE Controller 1		adapters as needed.		
OVD Drive				
DVD Drive DDEI-3.5.0-1058-x86_6				
DVD Drive DDEI-3.5.0-1058-x86_6 SCSI Controller	-			
DVD Drive DDEI-3.5.0-1058-x86_6 SCSI Controller  Network Adapter	-	c		
DVD Drive DDEI-3.5.0-1058-x86_6 SI SCSI Controller  Network Adapter Management Switch	-	r		
DVD Drive DDEF-3.5.0-1058-x86_6 SI SCSI Controller SI Network Adapter Management Switch COM 1		n Victual machines are arreated with or activities are model.		
DVD Drive DDE-3-1058-x86_6     SCSI Controller     Management Switch     COM 1     None	-	e Motod maddens are presided with an		
DVD Drive DDE7-3.5.0-1058-x86_6     Sill SCSI Controller Management Switch COM 1 None COM 2 COM 2 Veter State	-	ur		
DVD Drive DDEF-3.5.0-1058-x86_6     DEF-3.5.0-1058-x86_6     Solution     Coll 1     Anagement Switch     COM 1     None     COM 2     None     Odd 1     Defente Defen		n		
DVD Drive DDE7-3.50-1058-x86_6     DDE7-3.50-1058-x86_6     Solution     COM J Solution     COM 1     None     COM 1     None     COM 2     None     Diskette Drive     None		r		
DVD Drive DDE-3-01058-x86_6     SCSI Controller Management Switch COM 1 None COM 2 None Diskette Drive None Diskette Drive None	-	e		
DVD Drive DDE1-3.5.01058-x86_6     DE1-3.5.01058-x86_6     Sill SCSI Controller Management Switch COM 1 None COM 2 None Diskette Drive None None Com 2 None Diskette Drive None T Name		n		
DVD Drive DDE7-3.50-1058-x86_6      DE7-3.50-1058-x86_6      Solution     Controller      Management Switch      COM 1     None      COM 2     None      Diskette Drive     None      X Management      Name     Deep Discovery Email Inspector		n		
DVD Drive     DDEF-3.5.0-1058-x86_6      DVD Drivel     DDEF-3.5.0-1058-x86_6      DVD Drivel     Management Switch     COM 1     None     COM 2     None     Diskette Drive     None     Diskette Drive     None     Deep Discovery Email Inspector     Deep Discovery Email Inspector     Integration Services		r		
DVD Drive DDE2-30-1058-x86_6     SCSI Controller Management Switch COM 1 None Diskette Drive None Diskette Drive Diskette Dr		er		
DVD Drive DDE7-3.5.0-1058-x86_6     DVD Drive DDE7-3.5.0-1058-x86_6     Signal Controller Nonce COM 1 None COM 2 None Diskette Drive None Diskette Drive None Deep Discovery Email Inspector Changement Name Deep Discovery Email Inspector Dervices offered Checkpoints		n		
DVD Drive     DDE7-3.5.0-1058-x86_6      DVD Drive     DDE7-3.5.0-1058-x86_6      Softwork Adapter     Management Switch     COM 1     None     COM 2     None     Diskette Drive     None     Diskette Drive     None     Dekette Drive		n		
DVD Drive DDE-3-01058-x86_6     SCSI Controller Management Switch COM 1 None COM 2 None Diskette Drive None Diskette Drive None Management Integration Services Some services offered Checkpoints Production Smart Paging File Location				

m. Click Add.

The Network Adapter settings appear.

n. For Virtual switch, select Data Switch.



o. Click Apply.

p. Click OK.

## **Creating a Virtual Machine using KVM**

This section shows you how to create a virtual machine using KVM on Centos 7.9.

#### Procedure

**1.** On the KVM host, create a network bridge for virtual machine communication. Do the following:

- **a.** Open the network file /etc/sysconfig/network-scripts/ifcfgens192 using a text editor and make the following edits:
  - Comment out the line for BOOTPROTO
  - Add BRIDGE=br1

The following shows a file example.



**b.** Create a new network file /etc/sysconfig/network-scripts/ ifcfg-br1 with the following content:

DEVICE=br1 BOOTPROTO=static ONBOOT=yes TYPE=Bridge

a. Restart the network service.

File Edit View Help     Add Connection   New Virtual Machine   Close Ctrl+W   Quit Ctrl+Q     Close   Ctrl+Q	×
Add Connection   New Virtual Machine   Close   Ctrl+W   Quit   Ctrl+Q	
New Virtual Machine     CPU usage       Close     Ctrl+W       Quit     Ctrl+Q	
Close Ctrl+W Quit Ctrl+Q	
Quit Ctrl+Q	
Running	
	~

2. Open Virtual Host Manager and click **File** > **New Virtual Machine**.

**3.** On the New VM screen, select **Local install media (ISO image or CDROM)** and click **Forward**.

		New	VM		×
2	Create Step 1 (	a new virtu of 5	al machine		
Conne	ction: QE	MU/KVM			
Choos	e how yo	u would like to	o install the op	perating sy	stem
$\odot$	Local inst	all media (ISO	image or CDF	ROM)	
0	Network	Install (HTTP,	FTP, or NFS)		
0	Network	Boot (PXE)			
0					
0	Import ex	isting disk ima	ige		
0	Import ex	isting disk ima	ige		
0	Import ex	isting disk ima	ige		
0	Import ex	isting disk ima	lge		

**4.** Select **Use ISO image** and click **Browse** to select the Deep Discovery Email Inspector installation ISO image; then, click **Forward**.

	New VM	×
Crea Step	ate a new virtual machine 2 of 5	
Locate your	install media	
🔿 Use C	DROM or DVD	
No m	edia detected (/dev/sr0) 👻	
• Use IS	O image:	
/var/li	b/libvirt/images/DDEI-Rocky9-5-1-	rowse
Automat	ically detect operating system based on install	media
OS type:	Linux 👻	
Version:	Red Hat Enterprise Linu 👻	
	Cancel Back I	Forward

**5.** Configure the memory and CPU resource settings for the virtual machine and click **Forward**.



	New	VM		×
Create a r Step 3 of 5	new virtu	al ma	chine	
Choose Memory an	nd CPU set	tings		
Memory (RAM):	10240	<u></u>	+	
	Up to 32006	MiB av	ailable o	n the host
CPUs:	3	3-	+	
	Up to 40 ava	ilable		
0	ancel	D	ack	Ecoupred

**6.** Configure the storage setting and click **Forward**.

<ul> <li>Create a dis</li> </ul>	sk imag	e for	the virtua	l mach	nine
500.0	-	+	GiB		
41.3 GB av Select or cl	reate ci	ustor	n storage	ocatiol	1
Manage					

**7.** Specify the name (for example, "Deep Discovery Email Inspector") for the new virtual machine and select the network bridge you created; then, click **Finish**.

Ste			
Ready to be	gin the installation		_
Name:	Deep Discovery E	mail Inspecto	r
OS:	Generic		
Install:	Local CDROM/ISO		
Memory:	1024 MiB		
CPUs:	1		
Storage:	20.0 GiB eep Disco	overy Email Inspe	ector.qcow2
	Customize con	figuration bef	ore install
✓ Network	selection		
Bridge	br1: Host device e	ns192 🕶	

# **Creating a Virtual Machine on Nutanix AHV**

This section shows you how to create a virtual machine on Nutanix AHV.



#### Procedure

- **1.** Access the Nutanix Prism Element web console to upload the Deep Discovery Email Inspector installation ISO image. Do the following:
  - a. On the Settings dashboard, select Image Configuration and click Upload Image.

👝 jenny_cluster   Settings 🔹   😂 🐥 2 + 🔿 ×					
ettings	Image Configuration				
neral Australia	Manage the images to be used for creatin	g virtual disks.			
Infigure CVM	Name Annotation	Type	State	Size	
pand Cluster	centos7	ISO	ACTIVE	9.5 GiB	× · ×
age Configuration	ddel iso	ISO	ACTIVE	3.83 GiB	2 · ×
boot					
grade Software					
and the second se					
nnect to Citrix Cloud					
ism Central Registration					
lse					
ck Configuration					

#### The Create Image screen appears.

**b.** Type a descriptive name (for example, "Deep Discovery Email Inspector").

Create Image	?
Name	
Annotation	
Image Type	
ISO	]
Storage Container	_
default-container-87691031370460 ~	
Image Source	
○ From URL	
• Upload a file ③ Choose File No file chosen	
Gancel     Save	

- c. Select ISO from the Image Type drop-down list.
- **d.** Select **Upload a file** and click **Choose File** to select the Deep Discovery Email Inspector installation ISO image.
- e. Click Save.
- **2.** Create a new subnet. Do the following:
  - a. On the Settings dashboard, select Network Configuration and click Subnets.

Na jenny_cluster Se	ettings ~		<b>≜ 2</b> •	0 •		Q ? ~	🕸 admin 🖌
Settings	Network Conf	iguration					?
HTTP Proxy Name Servers	Subnets	Internal Ir	iterfaces	Virtual Swit	ch		+ Create Subnet
Network Configuration	Subnet Name	Virtual Switch	VLAN	Used IP Addresses	Free IPs in Subnets	Free IPs in Pool	Actions
NTP Servers	sub1	vs0	0	N/A	N/A	N/A	Edit · Delete
	sub2	vs0	1	N/A	N/A	N/A	Edit Delete
Security Cluster Lockdown	sub3	vs0	0	N/A	N/A	N/A	Edit Delete
Data-at-rest Encryption							

### **b.** Click **Create Subnet**.

**c.** On the **Create Subnet** screen, type a descriptive name and type "0" for the VLAN ID; then, click **Save**.

eate Subnet	
Subnet Name	
Subnet1	
Virtual Switch	
vs0	v
VLAN ID 🛞	
0	
Enable IP address management	
This gives AHV control of IP address assignments within the network.	
	Cancel

3. Go to the VM dashboard and click Create VM.

No jenny_cluster VM	· · · • + 0 ·											🗘 🕴 admin 🗸
Overview · Table										+ Cr	sate VM	Network Config
VM							Include	Controller VMs -	No entities found (filter	ed from 3) 🏮 · 🗘 ~ ·		
- VM Name Ho	st P Add	cores	Memory Capacity	Storage	CPU Usage	Memory Usage	Controller Read IOPS	Controller Write IOPS	Controller 10 Bandwidth	Controller Avg IO Latency	Backup a	Flash Mode

4. On the **Create VM** screen, do the following:

Create VM	?	×
General Configuration		1
Name		
Deep Discovery Email Inspector		
Description		
Optional		
Timezone		
(UTC) UTC	~	
Jse UTC timezone for Linux VMs and local timezone for Windows VMs.		
Use this VM as an agent VM		
Compute Details		
/CPU(s)		
3		

- **a.** Type a descriptive name (for example, "Deep Discovery Email Inspector").
- **b.** Allocate 3 or more vCPUs for the virtual machine.
- c. Allocate 10G or more memory for the virtual machine.
- **d.** Under **Disk**, click the edit button to update the CD-ROM settings.
- e. On the **Update Disk** screen, select the **Clone from Image Service** operation and select an image; then, click **Update**.

	Update Disk	? ×
The CD-ROM is empty		×
Туре		
CD-ROM		*
Operation		
Clone from Image Se	ervice	۰
Bus Type		
IDE		~
Image 🛞		
ddei iso		~
Size (GiB) 🕐		
Please note that changing	the size of an image is not allowed.	
Index		
0 (in use)		*
	Canc	el Update

**f.** Click **Add New Disk**, select the **SATA** bus type and allocate at least 500GB disk size; then click **Add**.

Add Disk		? ×
Туре		
DISK		•
Operation		
Allocate on Storage Container		~
Bus Type		
SATA		•
Storage Container		
default-container-87691031370460 (31		•
Size (GiB) 🕐		
500		
Index		
Next Available		•
	Cancel	Add

**g.** Under **Network Adapters (NIC)**, Click **Add New NIC** and select the subnet you have created; then click **Add**.

	Create NIC	? ×
Subnet Name		
Subnet1		~
Network Connection State		
Connected		Ť
Private IP Assignment		
NONE		

h. Click Save.

6-46

The **VM** dashboard displays an entry for the new virtual machine.

**5.** Install Deep Discovery Email Inspector on the new virtual machine. Eject the CD-ROM and reboot.

For more information, see the Nutanix documentation.


7-1

# **Chapter 7**

# **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

- 1. Go to https://success.trendmicro.com.
- **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:

https://success.trendmicro.com/srf/SRFMain.aspx

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 <u>http://about-threats.trendmicro.com/us/threatencyclopedia#malware</u> 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	https://www.trendmicro.com
Email address	support@trendmicro.com

• Worldwide support offices:

https://www.trendmicro.com/us/about-us/contact/index.html

- ※
  - \*
- Trend Micro product documentation:

# https://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:

https://success.trendmicro.com/solution/en-US/1112106.aspx

# **File Reputation Services**

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

https://success.trendmicro.com/solution/en-us/1059565.aspx

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**

7-6

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:

https://docs.trendmicro.com/en-us/survey.aspx



# Index

# A

about deployment, 2-2 administration, 5-2, 5-3, 5-5, 5-6 back up settings, 5-5, 5-6 product upgrades, 5-2, 5-3 restore settings, 5-5, 5-6

#### В

backup, 5-5, 5-6

## С

certificate management, 1-2 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, 3-17, 3-19

#### D

deployment installation, 3-10 network topology, 2-3 overview, 2-2 system requirements, 3-2 deployment tasks installation, 3-11 documentation feedback, 7-6 Download Center, 5-2, 5-3

### Е

enter CLI, 4-1 Ethernet cables, 2-10 export settings, 5-6

## F

firmware update, 5-3

### G

getting started management console, 3-19 management console access, 3-17

## I

iDRAC, 3-11 installation, 3-11 import settings, 5-6 installation, 3-2 network topology, 2-3, 2-4, 2-6 operating system, 3-10 Integrated Dell Remote Access Controller (iDRAC), 3-11 Intranet, 2-10

### М

Malware Lab Network, 2-9 management console, 3-17, 3-19 management network, 2-9 minimum requirements, 3-2

#### Ν

network environment, 2-9 network topology, 2-3

### 0

operation modes BCC mode, 2-3 MTA mode, 2-4 SPAN/TAP mode, 2-6

## Ρ

patches, 5-3 ports, 3-5 product upgrade, 5-2, 5-3

#### R

requirements, 3-2 restore, 5-5, 5-6

## S

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

## Т

test network, 2-10

## U

using CLI, 4-1



#### TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A. Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736 Email: support@trendmicro.com



Item Code: APEM59195/210115