TREND MICRO™

5.1 TREND MICRO™ Deep Discovery™ Email Inspector

Installation and Deployment Guide

Advanced Protection Against Targeted Email Threats

Endpoint Security

Network Security

Protected Cloud

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 docs@trendmicro.com.

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

Chapter 4: Using the Command Line Interface

Chapter 5: Upgrading Deep Discovery Email Inspector

Chapter 6: Creating a New Virtual Appliance

Chapter 7: Technical Support

Index

Preface

Preface

Topics include:

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: https://success.trendmicro.com

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, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	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™ 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® 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. https://www.trendmicro.com

Chapter 1

Introduction

Topics include:

About Deep Discovery Email Inspector

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

What's New

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

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	Deep Discovery Email Inspector provides the email address modification feature that allows you to: • Rewrite sender or recipient addresses in message envelops or message headers • Rewrite domains in email addresses

Feature	Description
Enhanced TLS communications	TLS communications has been enhanced in Deep Discovery Email Inspector to support the following: • TLS 1.3 • Secure connections for message transfer based on specified domains and IP addresses
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: • Send a blind carbon copy (BCC) of detected messages to specified recipients • Change the recipients of detected messages • Configure sender-recipient exceptions in policies • Configure address groups as policy objects • Internal email spoofing prevention • Apply message stamps based on policy rules
Sender and recipient validation for Inbound messages	Deep Discovery Email Inspector provides the following security settings to enhance inbound message security: • Reject messages from unknown sender IP addresses or domains • Reject messages to unknown recipients • Match message header FROM address for sender filtering
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 • Syslog forwarding for detected URLs

Feature	Description
Enhanced Virtual Analyzer	The Virtual Analyzer has been enhanced to include the following features: • Open Document file type for sandbox analysis • Windows 10 20H1 image support
Improved detection capability	Deep Discovery Email Inspector provides increased protection by improving its detection capabilities. This release supports the following: • ALG and EGG archive files for scanning • Decryption of password-protected ALG and EGG archive files and Open Document files for scanning • URL extraction from Open Document files for scanning • DLP forensic data display on the Detections screens
Enhanced approved and blocked senders lists	Configuration of the approved and blocked senders lists has been enhanced to include the following: • Sender list import and export • 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.

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

Chapter 2

Deployment

Topics include:

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.

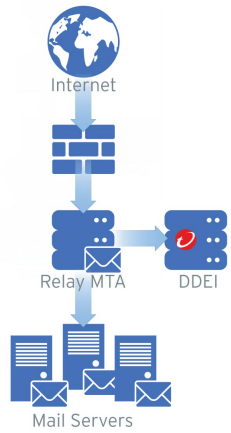


FIGURE 2-1. BCC Mode

MTA Mode

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.

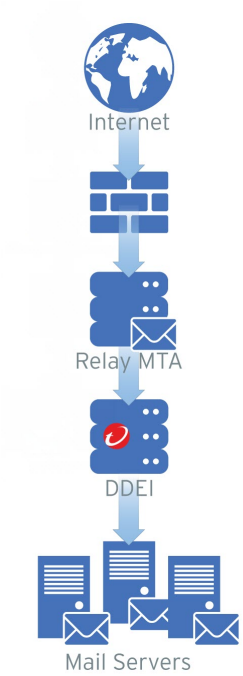


FIGURE 2-2. Non-edge MTA

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.

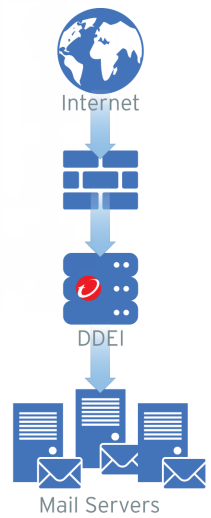


FIGURE 2-3. Edge MTA

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.

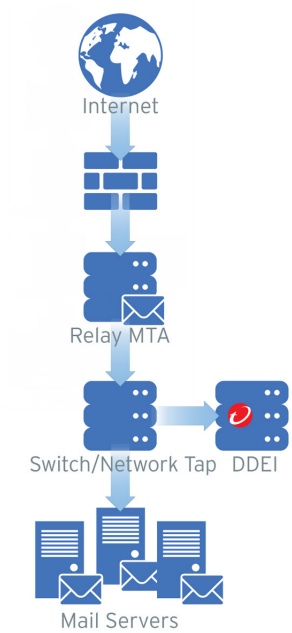


FIGURE 2-4. SPAN/TAP Mode

Note

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

Apex Central Deployment

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

The following figure shows how email messages pass through a network with multiple Deep Discovery Email Inspector appliances configured in MTA mode and registered to Apex Central. Each Deep Discovery Email

Inspector appliance independently processes email messages as an MTA while management is centralized through Apex Central.

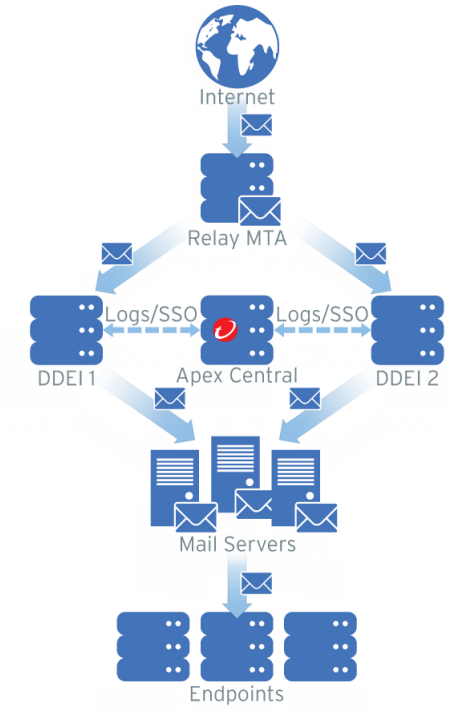


FIGURE 2-5. Apex Central Deployment

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

Recommended Network Environment

Deep Discovery Email Inspector requires connection to a **management network**. After deployment, administrators can perform configuration tasks from any computer on the management network.

Connection to a **custom network** is recommended to simulate malware behavior when connecting to the Internet. For best results, Trend Micro recommends an Internet connection without proxy settings, proxy authentication, and connection restrictions.

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

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

Items to Prepare

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	Connect to the management and data ports • Required: Management port (eth0) of the appliance to the management network • Recommended: Data port (eth1, eth2, or eth3) connects to the custom network • Optional: Unused data ports connect to the mail network for mail routing and monitoring

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

Chapter 3

Installation

Topics include:

System Requirements

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

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.

TABLE 3-1. Specifications for Virtual Appliance

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

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)
MTA	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.

TABLE 3-3. System Access Requirements

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 access the management console. Using the data port IP address you set during the initial configuration, specify the following URL: `https://[Appliance_IP_Address]:443`
Mozilla Firefox™	Version 75 or later	
Google Chrome™	Version 81 or later	

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.

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

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 System (SMS)	• 5.4 • 5.3

Ports Used by the Appliance

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

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

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

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

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

Port	Protocol	Function	Purpose
5274	TCP	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: • Send logs to syslog servers • Share threat intelligence with integrated products/services • Upload detection logs to SFTP servers • Communicate with and Check Point Open Platform for Security (OPSEC) • Connect to an LDAP server for third-party authentication and LDAP query

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 *Configuring Management Console Access on page 3-17*.

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 • KVM (Kernel-based Virtual Machine) For more information, see *Virtual Host Appliance Requirements on page 3-2*.

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

1. Download the Deep Discovery Email Inspector installation ISO file from the **License** screen on the Business Success Portal at https://success.trendmicro.com/dcx/s/license.
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**.
7. 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.

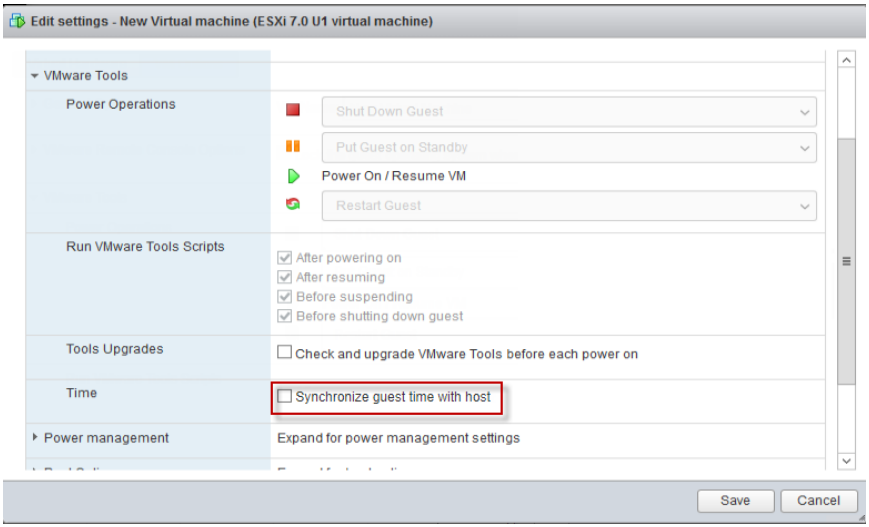
Procedure

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.



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.

   Note

   IPv6 settings are optional.

   - 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>
```

Note

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 https://success.trendmicro.com/dcx/s/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

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

Note

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

Entering the CLI

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

Procedure

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

    Note

    The default credentials are:

    - User name: `admin`
    - Password: `ddei`

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

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

Note

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

Command Line Interface Commands

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

Entering Privileged Mode

WARNING!

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

Procedure

1. Log on to the CLI.

   See *Entering the CLI on page 4-2*.

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

3. Type the default password, `trend#1`, and then press ENTER.

   The prompt changes from > to #.

CLI Command Reference

The following tables explain the CLI commands.

Note

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

configure product management-port

TABLE 4-1. configure product management-port

Set the management port IP address	
Syntax: `configure product management-port [ipv4 | ipv6] <ip> <mask>`	
View	Privileged
Parameters	**ipv4**: Configure IPv4 settings **ipv6**: Configure IPv6 settings **<ip>**: IP address for the interface **<mask>**: Network mask for the NIC
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>`	
View	Privileged

Parameters	**ipv4**: Configure IPv4 settings **ipv6**: Configure IPv6 settings **<dns1>**: Primary DNS server **<dns2>**: Secondary DNS server  **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>`	
View	Privileged
Parameters	**<hostname>**: The host name or fully qualified domain name (FQDN) for the Deep Discovery Email Inspector device
Examples:	
To change the host name of the Deep Discovery Email Inspector device to test.host.com: `configure network hostname test.example.com`	

configure network interface

TABLE 4-6. configure network interface

Configures the IP address for the network interface card (NIC).	
Syntax: `configure network interface [ipv4 | ipv6] <interface> <ip> <mask>`	
View	Privileged
Parameters	**ipv4**: Configure IPv4 settings **ipv6**: Configure IPv6 settings **<interface>**: NIC name **<ip>**: IP address for the interface **<mask>**: Network mask for the NIC
Example:	
To configure an NIC with the following values: • Interface: `eth0` • IPv4 address: `192.168.10.10` • IPv4 subnet mask: `255.255.255.0` `configure network interface ipv4 eth0 192.168.10.10 255.255.255.0`	

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

configure network route default

TABLE 4-9. configure network route default

Sets the default route	
Syntax: `configure network route default [ipv4 | ipv6] <gateway>`	
View	Privileged

Parameter	**ipv4**: Configure IPv4 settings **ipv6**: Configure IPv6 settings **<gateway>**: IP address of default gateway
Example:	
To set the default route for the Deep Discovery Email Inspector appliance: `configure network route default ipv4 192.168.10.1`	

configure network route del

TABLE 4-10. configure network route del

Deletes a route	
Syntax: `configure network route del [ipv4 | ipv6] <ip_prefixlen> <via> <dev>`	
View	Privileged
Parameters	**ipv4**: Configure IPv4 settings **ipv6**: Configure IPv6 settings **<ip_prefixlen>**: Destination network ID with format IP_Address/Prefixlen **<via>**: IPv4 address of the next hop **<dev>**: Device name
Example:	
To delete a route for the Deep Discovery Email Inspector appliance: `configure network route del ipv4 172.10.10.0/24 192.168.10.1 eth1`	

configure network route del default/default ipv6

TABLE 4-11. 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>`	
View	Privileged
Parameters	port: configure the SSH service port <port>: SSH service port number
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>]`	
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
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>`	
View	Privileged
Parameters	**<date>**: Set the date using the following format: **yyyy-mm-dd** **<time>**: Set the time with the following format: **hh:mm:ss**
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>`	
View	Privileged
Parameters	**<region>**: Region name **<city>**: City name
Example:	
To configure the Deep Discovery Email Inspector appliance to use the time zone for the following location: Region: America City: New York `configure system timezone America New_York`	

TABLE 4-21. Time Zone Setting Examples

REGION/COUNTRY	CITY
Africa	Cairo
	Harare
	Nairobi
America	Anchorage
	Bogota
	Buenos_Aires

Region/Country	City
	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	City
	Jerusalem
	Kabul
	Karachi
	Katmandu
	Krasnoyarsk
	Kuala_Lumpur
	Kuwait
	Magadan
	Manila
	Muscat
	Rangoon
	Seoul
	Shanghai
Asia (Continued)	Singapore
	Taipei
	Tehran
	Tokyo
	Yakutsk
Atlantic	Azores
Australia	Adelaide
	Brisbane
	Darwin
	Hobart

Region/Country	City
	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	City
	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>`	
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
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>`	
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
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: `start task postfix drop { <mail_id> | all }`	
View	Privileged

Parameters	**<mail_id>**: Specifies the message ID in the postfix queue to delete
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>`	
View	Privileged
Parameters	**<pid>**: The process ID
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	**[time]**: 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>`	
View	Privileged
Parameter	**<dest>**: Specifies the IPv4 address or host name to resolve
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

Parameters	**arp**: Displays the value returned by the Address Resolution Protocol (ARP) for the given address. **<address>**: FQDN or IP address that will be resolved with the Address Resolution Protocol (ARP). **connections**: Displays the current network connections of the Deep Discovery Email Inspector appliance. **dns**: Displays the DNS IP address of the Deep Discovery Email Inspector appliance. **dns ipv6**: Displays system DNS configuration for IPv6. **hostname**: Displays the host name of the Deep Discovery Email Inspector appliance. **interface**: 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 information for the address 10.2.23.41: `show network arp 10.2.23.41`	
To display the current network connections of the Deep Discovery Email Inspector appliance: `show network connections`	
To display the DNS configuration: `show network dns`	
To display system DNS configuration for IPv6: `show network dns ipv6`	
To display the host name of the Deep Discovery Email Inspector appliance: `show network hostname`	

To display the NIC status and configuration: `show network interface`
To display the IP address route table: `show network route`
To display system IPv4 route table: `show network route ipv4`
To display system default IPv4 gateway: `show network route default ipv4`
To display system default IPv6 gateway: `show network route default ipv6`

show kernel

TABLE 4-45. 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. **iostat**: Displays CPU statistics and I/O statistics for devices and partitions.
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 <enabled | server-address> | ssh | nscd]`	
View	Normal
Parameters	**nscd**: Displays the status of the name service cache daemon. **ntp enabled**: Displays the system NTP service status. **ntp server-address**: Displays the system NTP service server address. **ssh**: 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	**vm**: 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	**top**: Displays the status of the processes that are currently running and system related processes **stack**: Print a stack trace of a running process **itrace**: Trace the library call **trace**: Trace system calls and signals **pid**: The process id number

Examples:

To display the status of the processes that are currently running:
`show process`
To display the stack trace of process 1233:
`show process stack 1233`
To display the system call of process 1233:
`show process trace 1233`
To display the library call of process 1233:
`show process itrace 1233`

show product-info

TABLE 4-49. show product-info

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

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

show system

TABLE 4-50. 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. **timezone**: Displays the timezone settings. You can optionally specify the timezone information to view: • **continent**: Displays the system continent • **city**: Displays the system city • **country**: Displays the system country **uptime**: Displays how long the Deep Discovery Email Inspector appliance has been running. **version**: 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	**[time]**: Shuts down the Deep Discovery Email Inspector appliance after a specified delay in minutes.
Examples:	
To shut down the Deep Discovery Email Inspector appliance immediately: `shutdown`	

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

traceroute

TABLE 4-52. traceroute

Displays the tracking route to a specified destination.	
Syntax: `traceroute [-h hops] <dest>`	
View	Normal
Parameters	**[-h hops]**: Specifies the maximum number of hops to the destination. The minimum number is 6. **<dest>**: Specifies the remote system to trace
Examples:	
To display the route to IP address 172.10.10.1 with a maximum of 6 hops: `traceroute 172.10.10.1`	
To display the route to IP address 172.10.10.1 with a maximum of 30 hops: `traceroute -h 30 172.10.10.1`	

Chapter 5

Upgrading Deep Discovery Email Inspector

Topics include:

System Updates

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 http://downloadcenter.trendmicro.com.

You can install a patch file on Trend Micro using one of the following methods:

- The Deep Discovery Email Inspector management console

- Plan deployment from Deep Discovery Director. For more information, see the Deep Discovery Director documentation.

Procedure

1. Go to **Administration** > **Product Updates** > **Hotfixes / Patches**.
2. Under **History**, verify the software version number.
3. Manage the product patch.
   - Upload a patch by browsing to the patch file provided by Trend Micro Support and then clicking **Install** under **Install Hotfix / Patch**.
   - Roll back a patch by clicking **Roll Back** under **History**. After rollback, Deep Discovery Email Inspector uses the most recent previous configuration. For example, rolling back patch 3 returns Deep Discovery Email Inspector to a patch 2 state.

Upgrading Firmware

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

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**.

Tip

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

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

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

Backing Up or Restoring a Configuration

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

Important

Deep Discovery Email Inspector only supports restoring configurations from other Deep Discovery Email Inspector servers with a compatible license status and with the same firmware version, hardware model, and locale. For example, you cannot restore a server running version 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*.

Note

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

Trend Micro recommends:

- Backing up the current configuration before each import operation

- Performing the operation when Deep Discovery Email Inspector is idle. Importing and exporting affects Deep Discovery Email Inspector performance.

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

License Compatibility

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

TABLE 5-2. License compatibility

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

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:

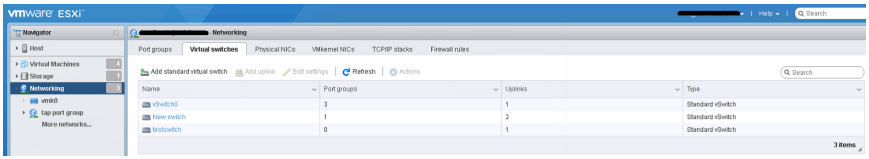
Configuring the VMware ESXi Server Network

Use a browser to connect the ESXi server.

Procedure

1. To log in to the VMware ESXi server, type a **User name** and **Password,** and then click **Log In**.

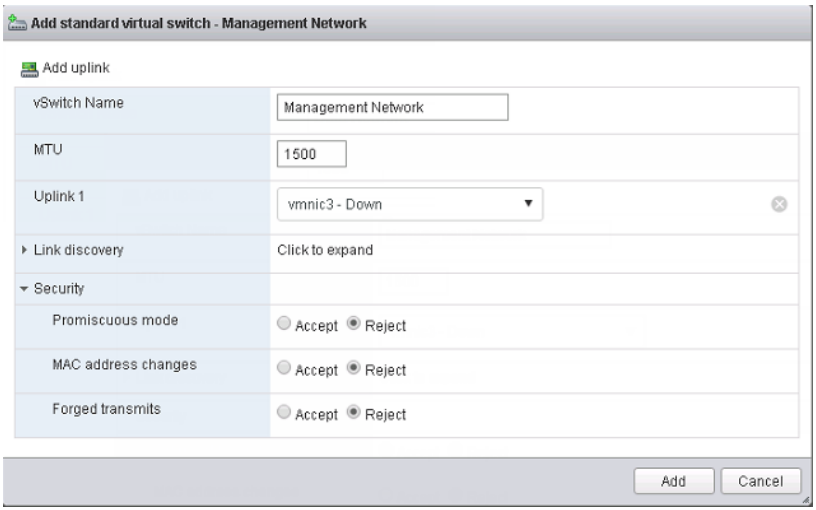
2. Click **Networking** and then click the **Virtual switches** tab. Observe the initial state.



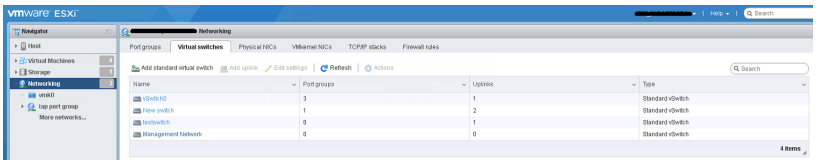
3. Click **Add standard virtual switches** and configure the following settings.

   a. For **vSwitch Name**, type a name (for example, Management Network).

   b. For **Uplink 1**, select a NIC card for **Management Network**.



   c. Click **Add**.



4. (Optional) Add a data network. On the **Virtual switches** tab, click **Add standard virtual switches** and configure the settings.

Note

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

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

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

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

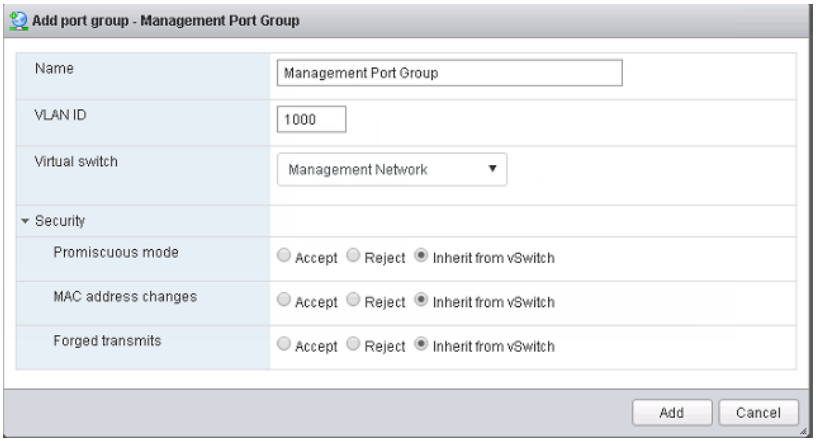
5. Click on the **Port groups** tab and observe the initial state.

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

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

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

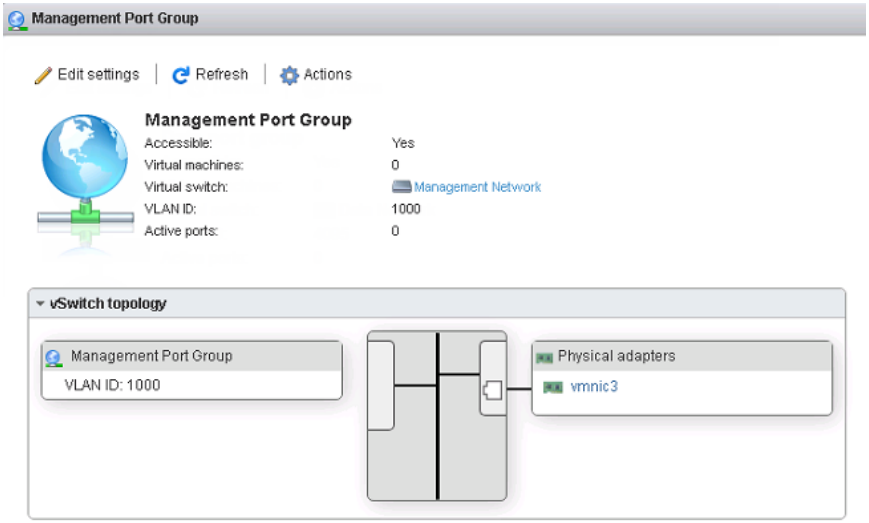
   c. For **Virtual switch**, select **Management Network**.



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

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

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

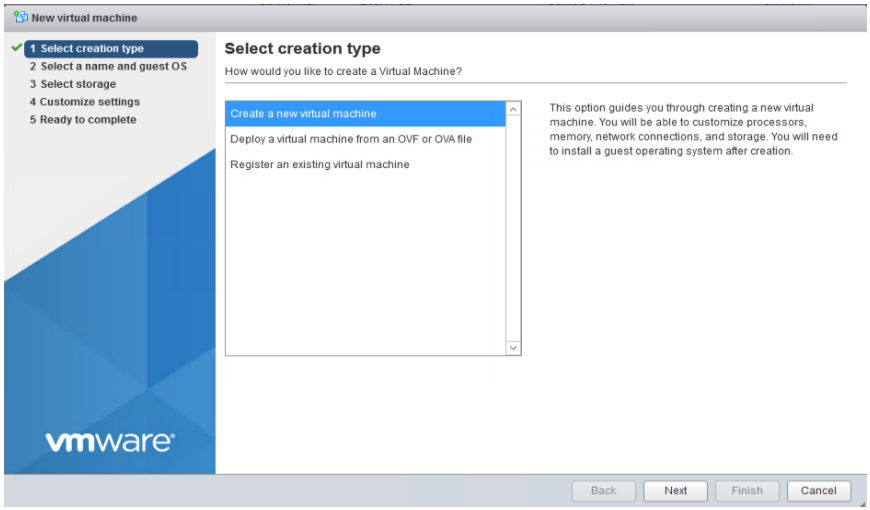


Creating a Virtual Machine in VMware ESXi

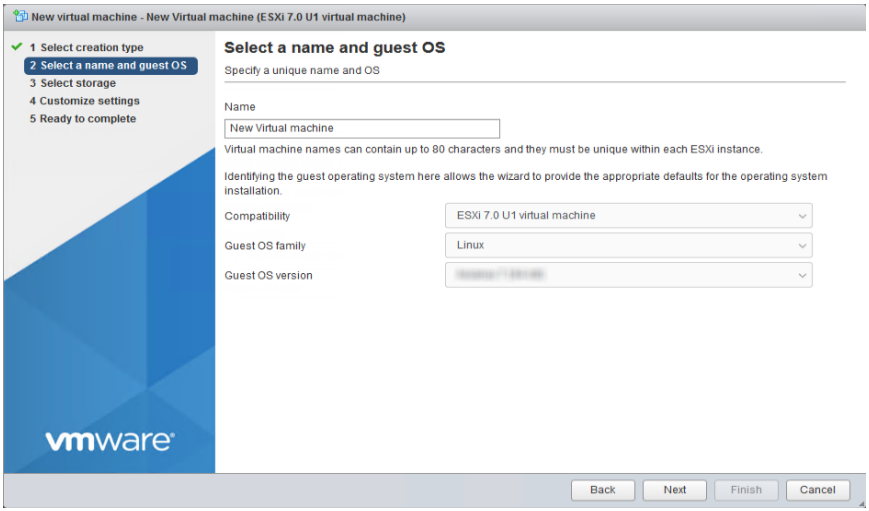
The following procedure is for VMware.

Procedure

1. Click **Virtual machines** and then click **Create / Register VM**.
2. On the **Select creation type** screen, click **Create a new virtual machine** and then click **Next**.

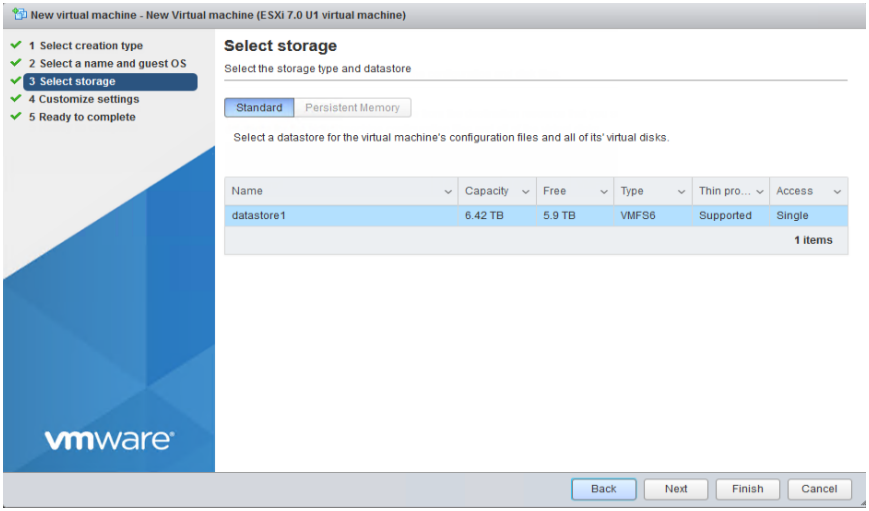


3. On the **Select a name and guest OS** screen, configure the settings.
   a. For **Name**, type `New Virtual Machine`.
   b. For **Compatibility**, select **ESXi 7.0 U1 virtual machine**.
   c. For **Guest OS family**, select **Linux**.
   d. For **Guest OS version**, select **CentOS 7 (64-bit)**.



4. Click **Next**.

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



6. Configure the settings on the **Customize settings** screen.

   a. For **CPU**, select the virtual CPU amount based on the throughput of your Virtual Deep Discovery Email Inspector license.

      - For 300K messages per day, select at least **3** virtual CPUs.
      - For 700K messages per day, select at least **6** virtual CPUs.

   b. For **Memory**, set the amount of memory based on the throughput of your Virtual Deep Discovery Email Inspector license.

      - For 300K messages per day, set at least **10 GB** of memory for the virtual machine.
      - For 700K messages per day, select at least **16 GB** of memory for the virtual machine.

   c. For **Hard disk**, set the amount of disk space based on the throughput of your Virtual Deep Discovery Email Inspector license.

      - For 300K messages per day, set at least **500 GB** of disk space for the virtual machine.
      - For 700K messages per day, select at least **1 TB** of disk space for the virtual machine.

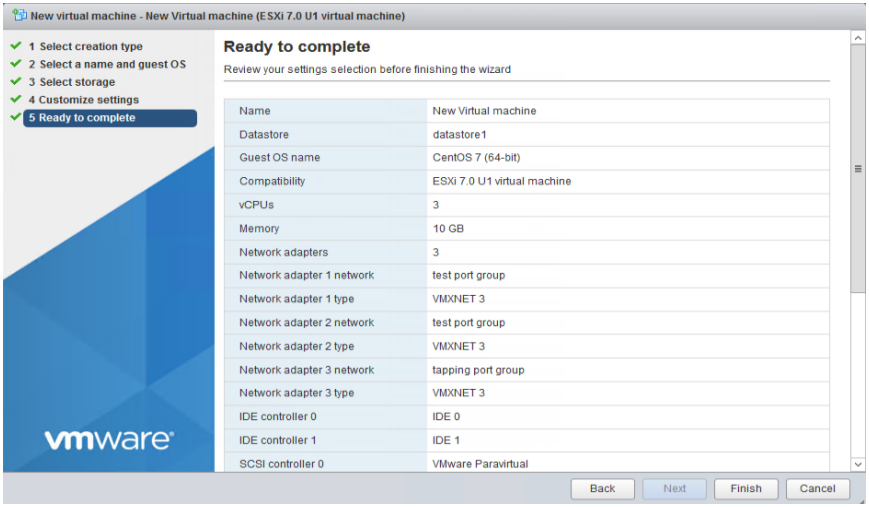
   d. For **Network**, configure the amount of NICs based on the function of your Virtual Deep Discovery Email Inspector license.

      - If Deep Discovery Email Inspector is set in MTA or BCC mode, configure at least 1 NIC.
      - If SPAN/TAP mode is enabled, configure at least 3 NICs with one each for the management and data networks.

        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**.

8. On the **Ready to complete** screen, review the settings and click **Finish**.

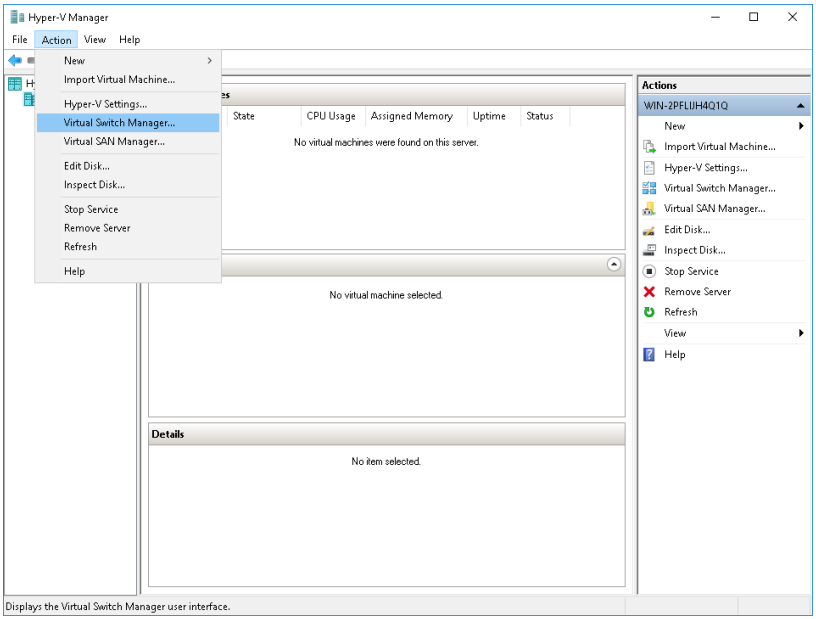


Creating a Virtual Machine in Microsoft Hyper-V

Procedure

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

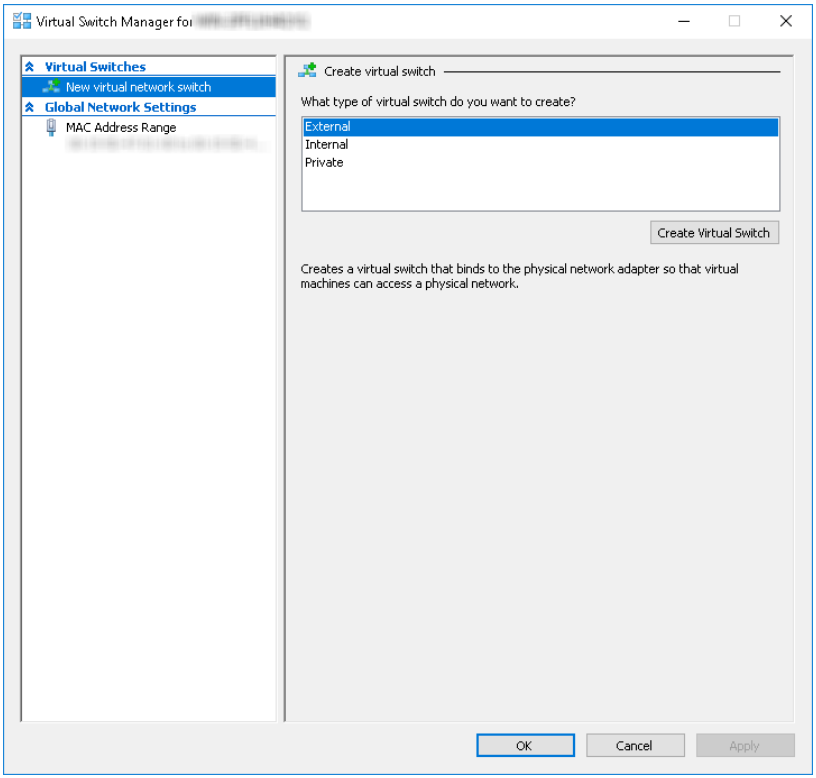
      The **Virtual Switch Manager** window appears.



b. In the left column, click **New Virtual network switch**.

The **Create virtual switch** screen appears.

c. For the switch type to create, select **External**.

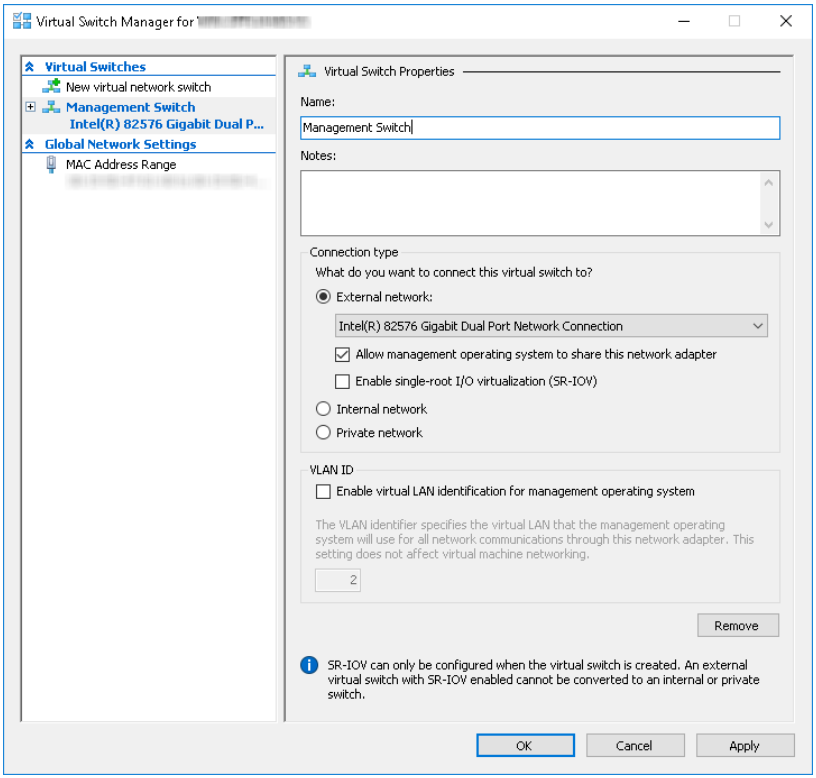


d. Click **Create Virtual Switch**.

The **Virtual Switch Properties** screen appears.

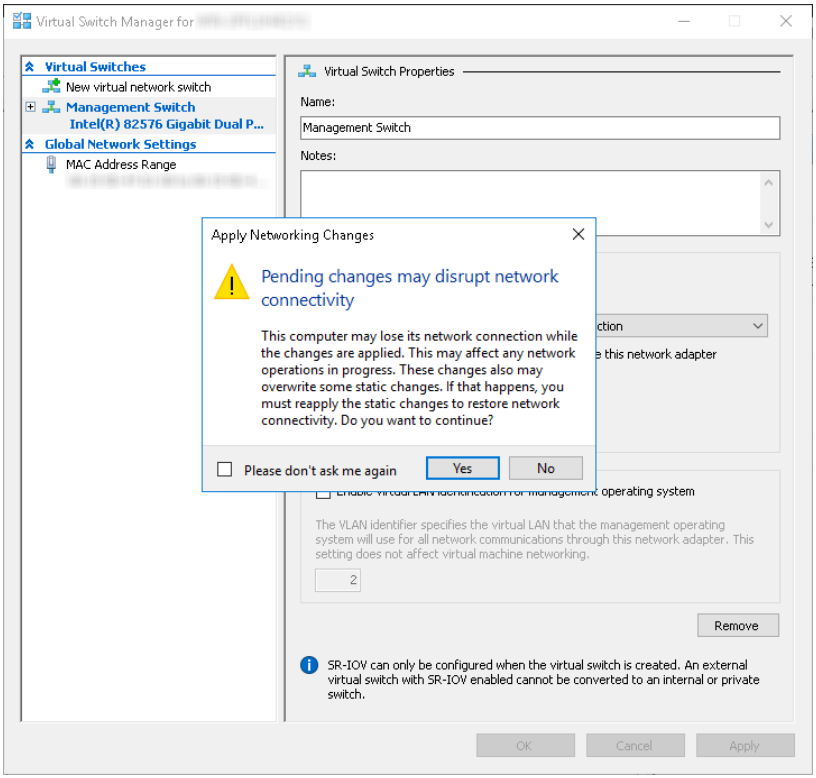
e. For **Name**, type `Management Switch`.

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



g. Click **Apply**.

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



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

i. In the left column, click **New Virtual network switch**.

The **Create virtual switch** screen appears.

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

k. Click **Create Virtual Switch**.

The **Virtual Switch Properties** screen appears.

l. For **Name**, type `Data Switch`.

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

n. Click **Apply**.

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

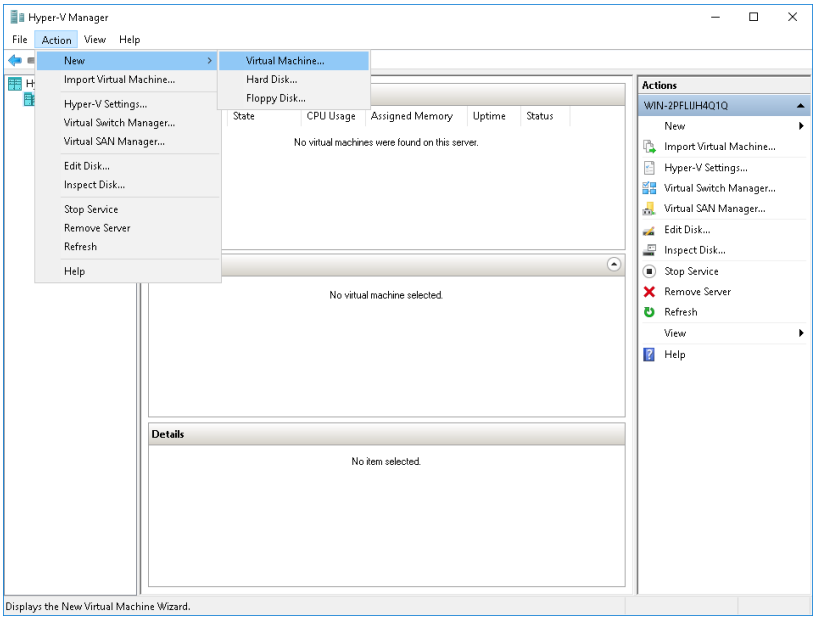
o. Read the warning and then click **Yes**.

The confirmation window closes.

p. Click **OK**.

2. Create a virtual machine.

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

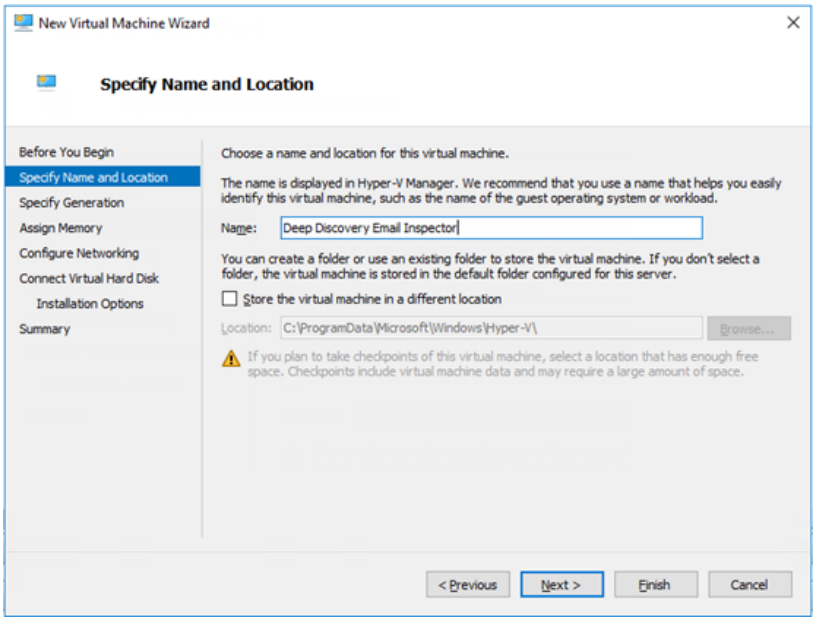


The **New Virtual Machine Wizard** window with the **Before You Begin** screen appears.

b. Click **Next**.

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

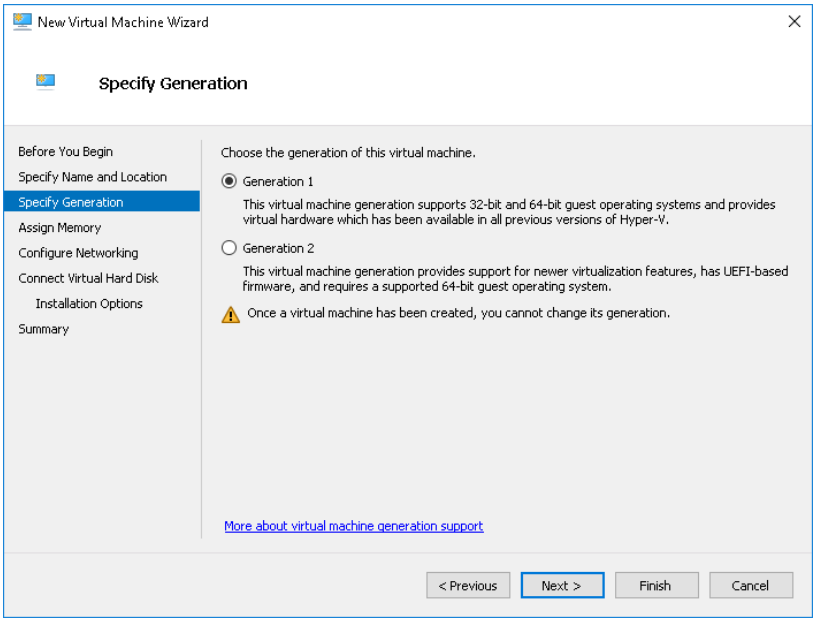
c. For **Name**, type `Deep Discovery Email Inspector`.



d. Click **Next**.

The **Specify Generation** screen appears.

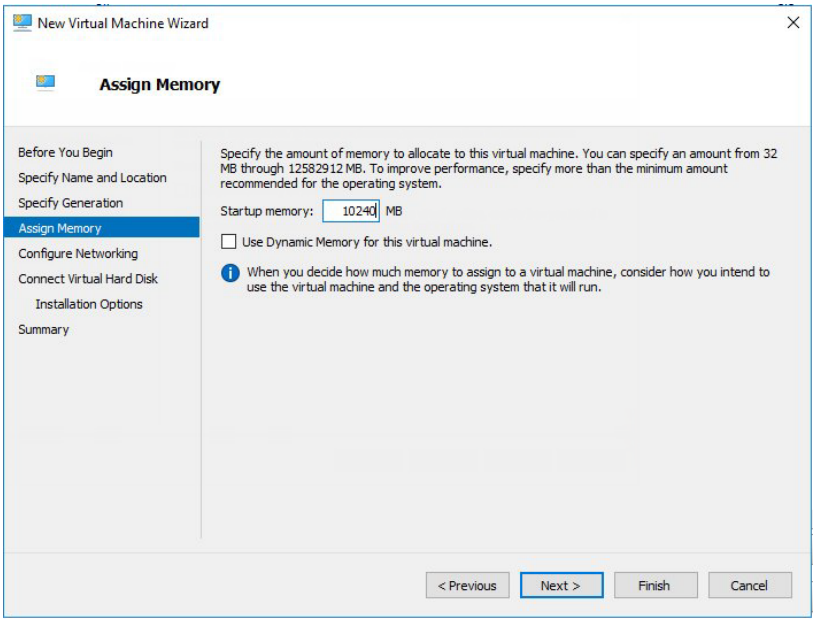
e. Select **Generation 1**.



f. Click **Next**.

The **Assign Memory** screen appears.

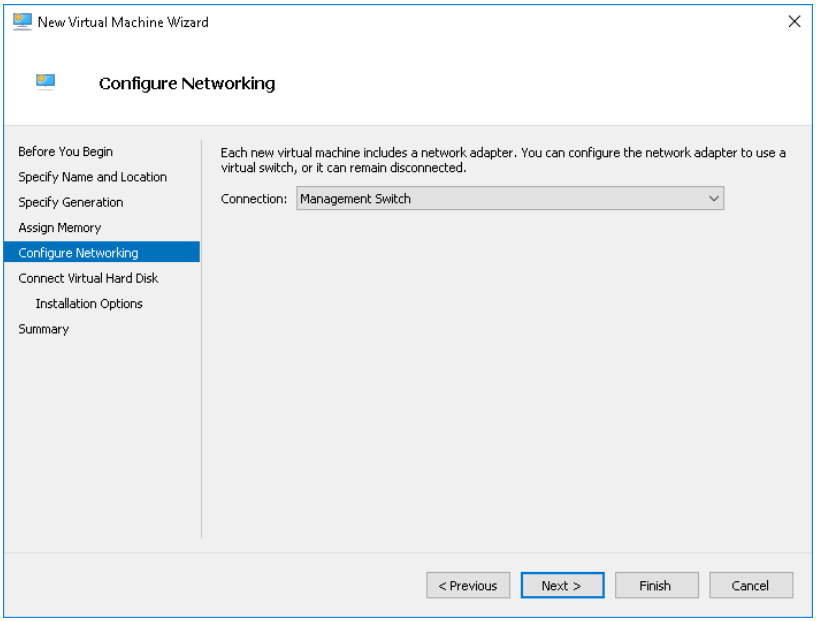
g. For **Startup memory**, assign at least `10240` MB (10 GB).



h. Click **Next**.

The **Configure Networking** screen appears.

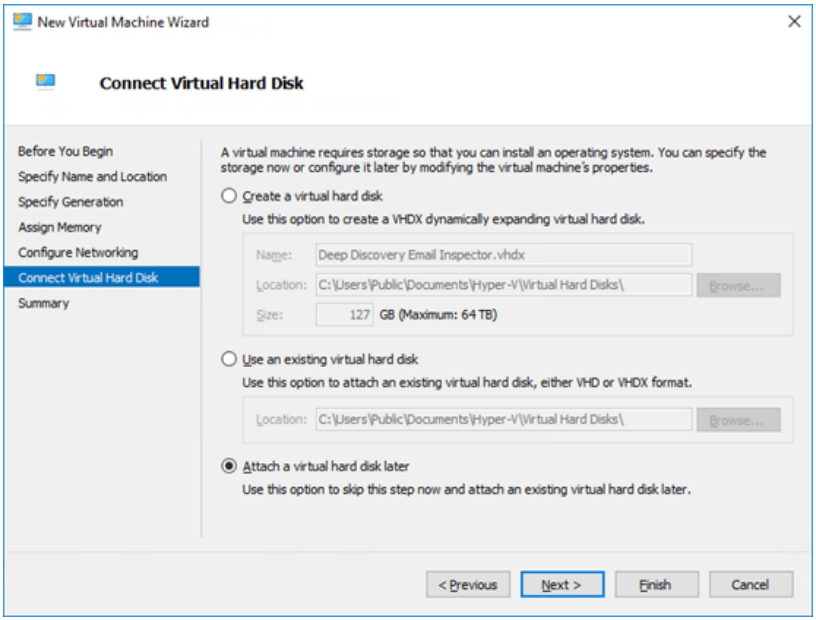
i. For **Connection**, select **Management Switch**.



j. Click **Next**.

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

k. Select **Attach a virtual hard disk later**.



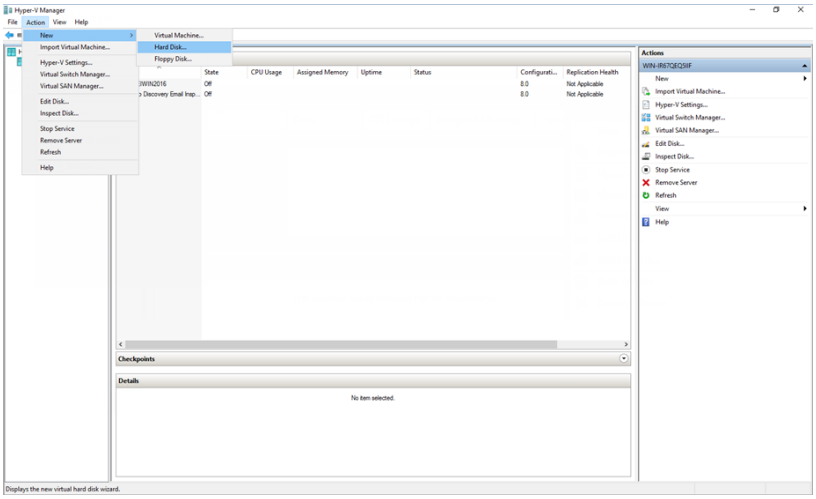
l. Click **Next**.

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**.

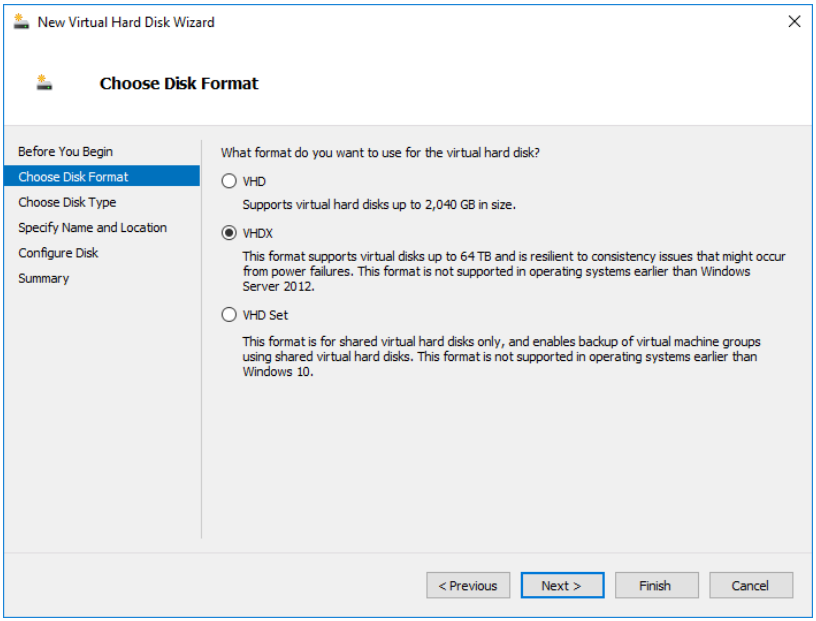


The **New Virtual Hard Disk Wizard** window with the **Before You Begin** screen appears.

b. Click **Next**.

The **Choose Disk Format** screen appears.

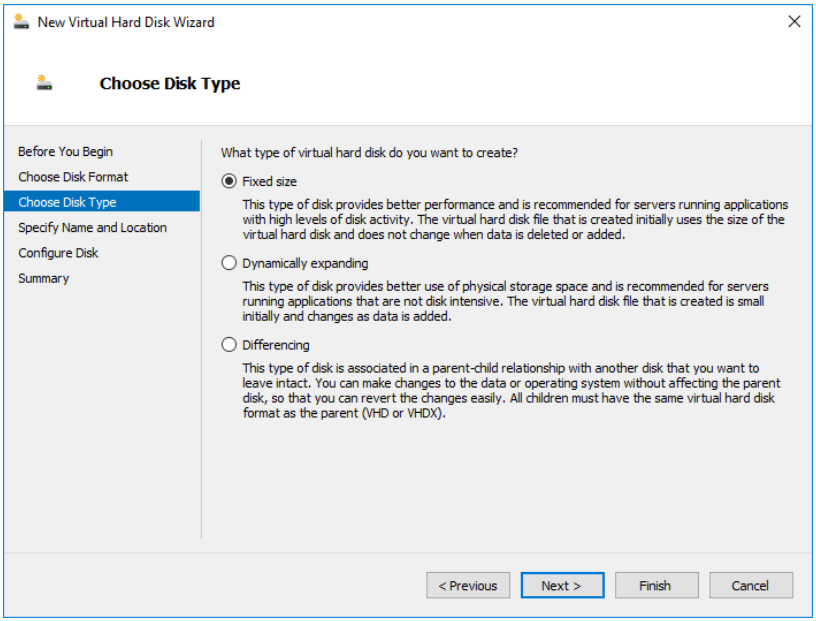
c. Select **VHDX**.



d. Click **Next**.

The **Choose Disk Type** screen appears.

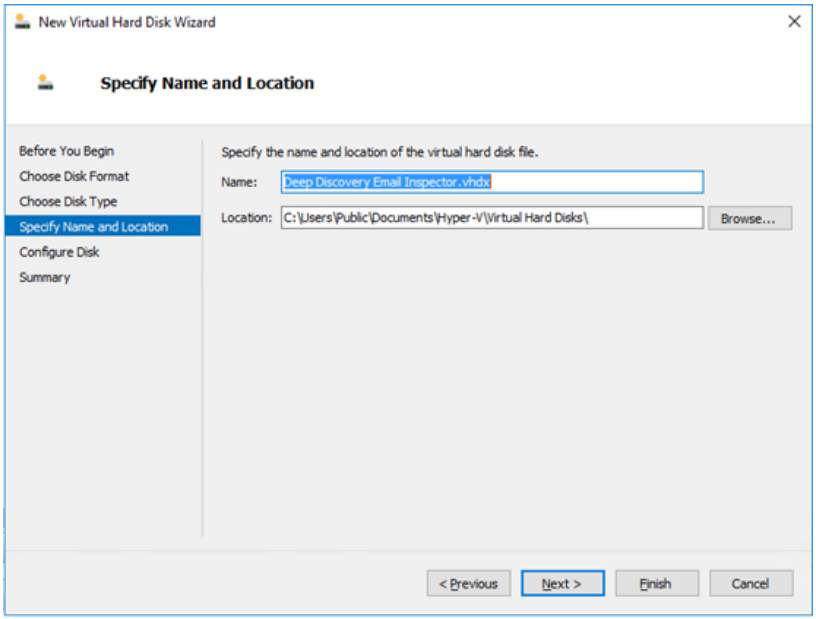
e. Select **Fixed size**.



f. Click **Next**.

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

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

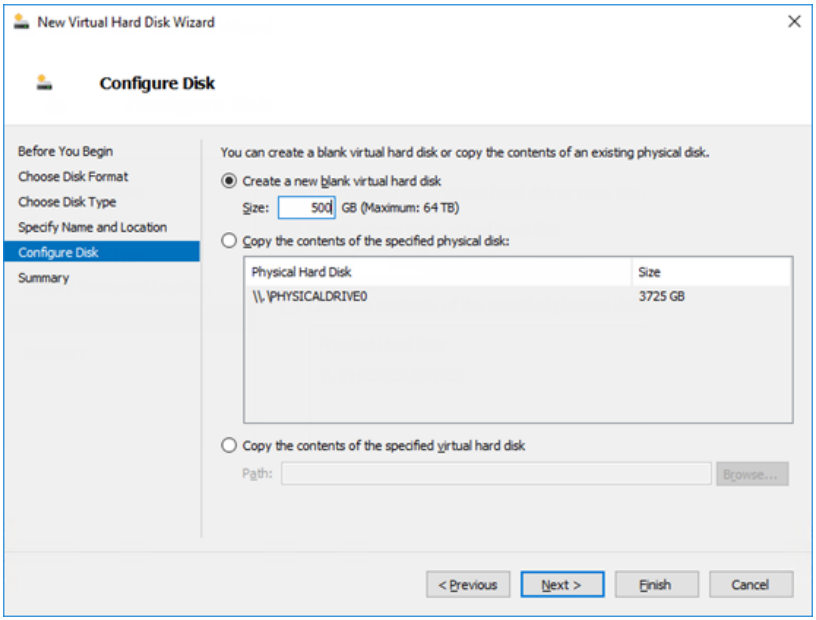


h. Click **Next**.

The **Configure Disk** screen appears.

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

j. For **Size**, specify at least `500` GB.



k. Click **Next**.

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

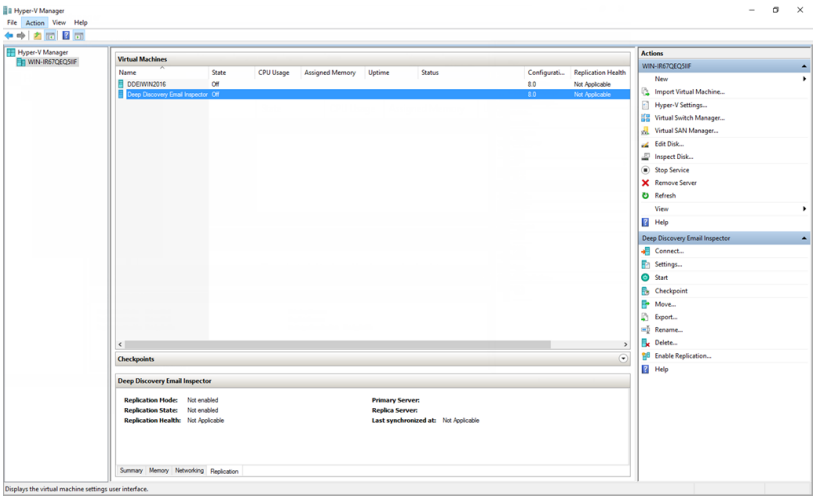
l. Verify that the hard disk configuration is correct and then click **Finish**.

Note

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

4. Configure the virtual machine.

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

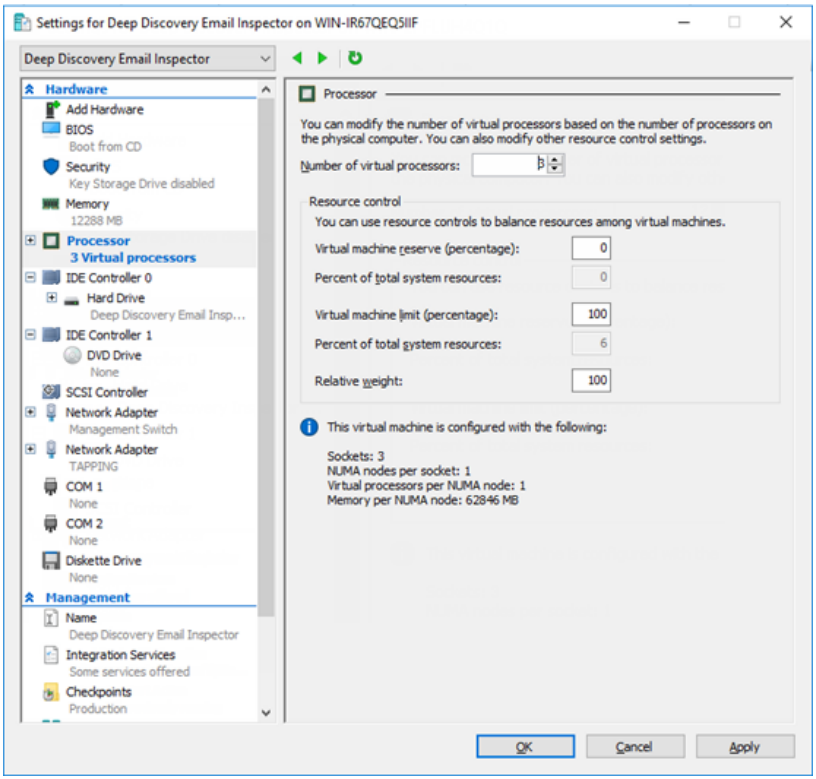


The settings window appears.

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

The **Processor** settings appear.

c. For Number of virtual processors, specify at least `3` virtual processors.

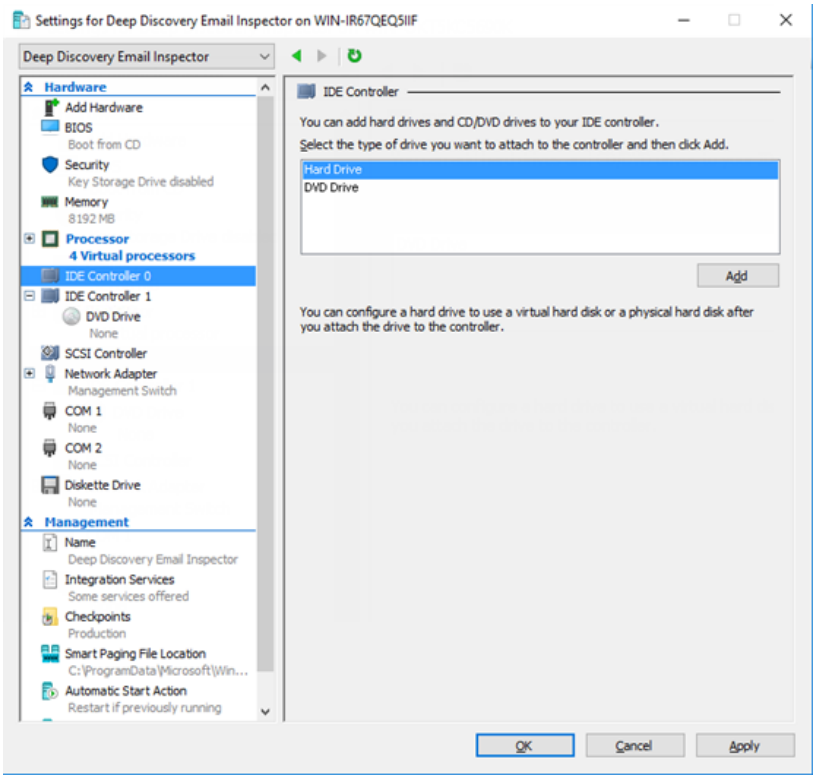


d. Click **Apply**.

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

The **IDE Controller** settings appear.

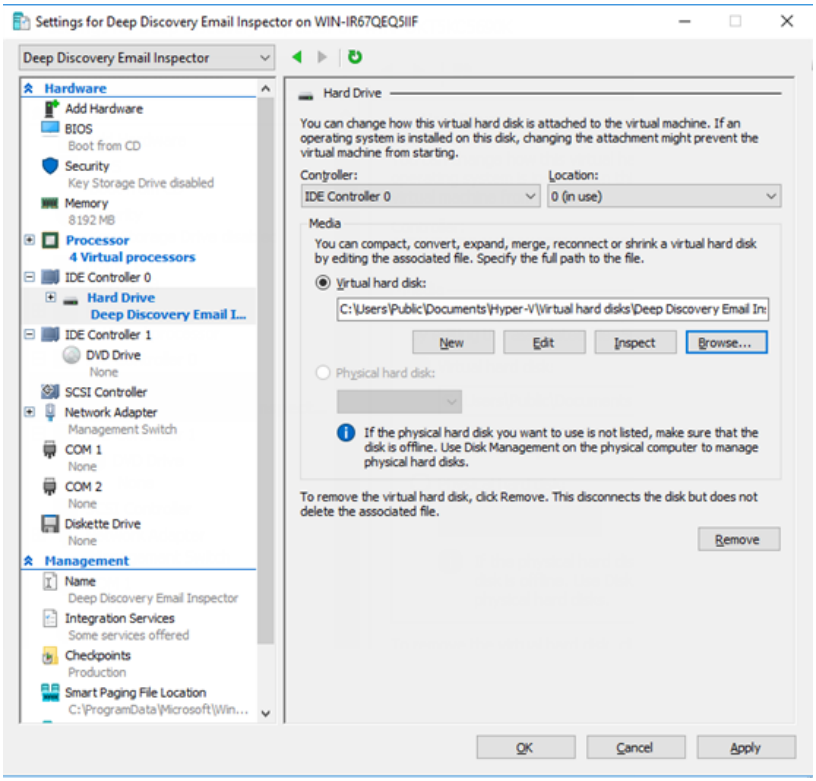
f. For the type of hard drive to attach to the controller, select **Hard Drive**.



g. Click **Add**.

The **Hard Drive** settings appear.

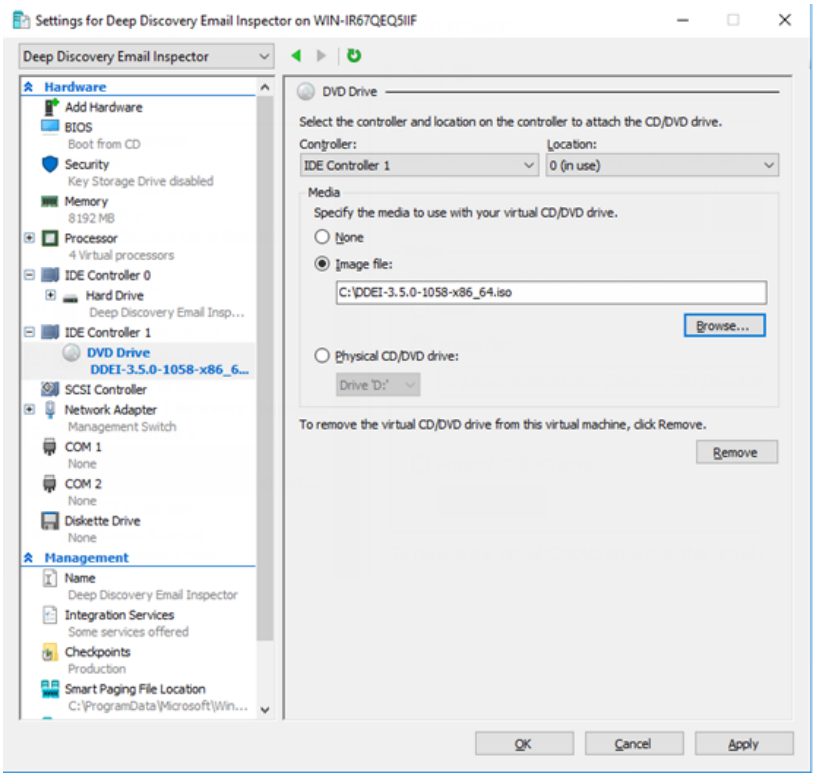
h. For **Virtual hard disk**, specify the location of `Deep Discovery Email Inspector.vhdx`.



i. In the left column, click **IDE Controller 1** and then click on **DVD Drive**.

The **DVD Drive** settings appear.

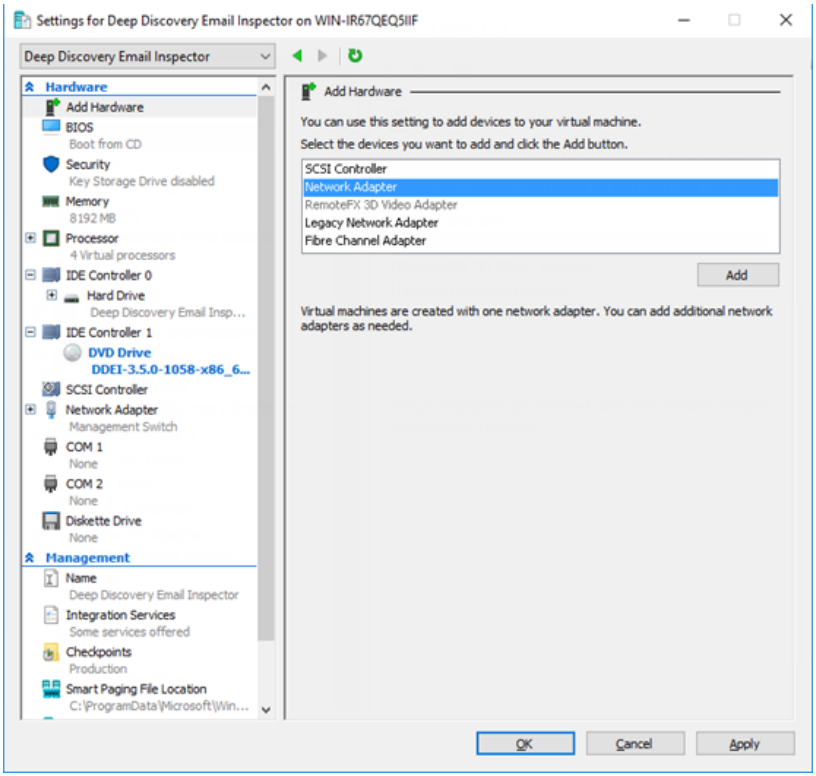
j. For **Media**, select **Image file** and then specify the location of the Deep Discovery Email Inspector ISO file.



k. In the left column, click **Add Hardware**.

The **Add Hardware** settings appear.

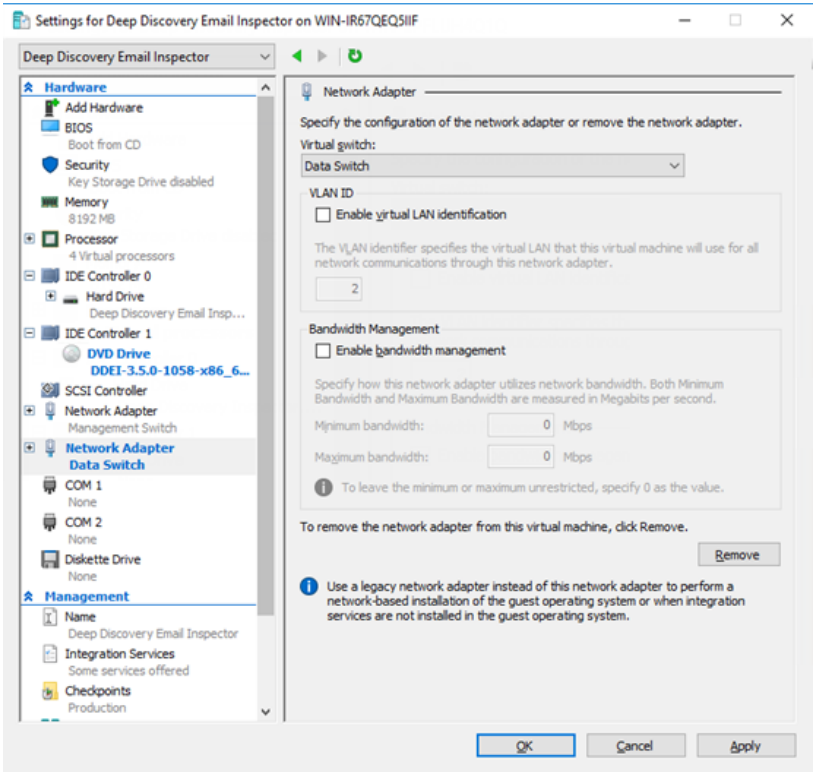
l. For the devices you want to add, select **Network Adapter**.



m. Click **Add**.

The **Network Adapter** settings appear.

n. For **Virtual switch**, select **Data Switch**.



o. Click **Apply**.

p. Click **OK**.

Creating a Virtual Machine using KVM

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

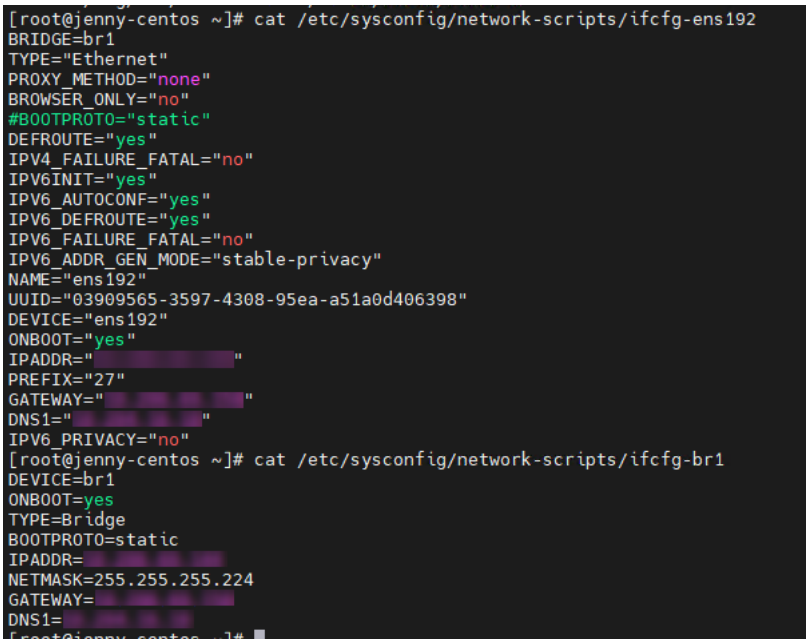
Procedure

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/ifcfg-ens192` using a text editor and make the following edits:

- Comment out the line for `BOOTPROTO`
- Add `BRIDGE=br1`

The following shows a file example.

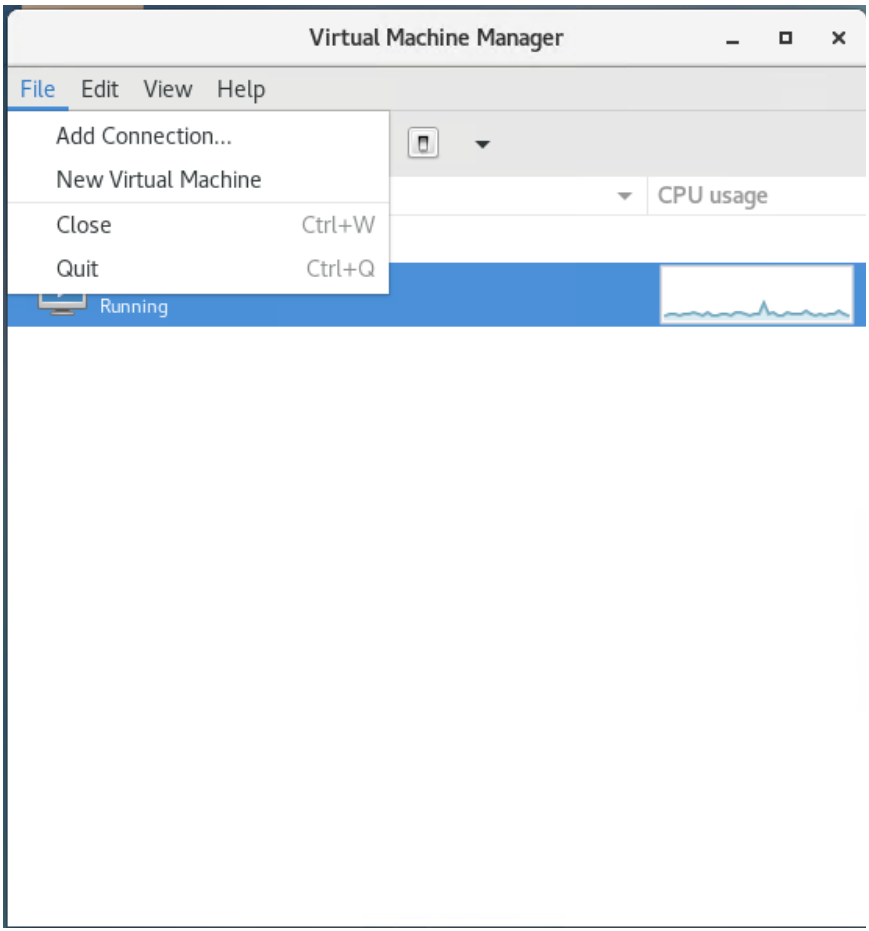


b. Create a new network file `/etc/sysconfig/network-scripts/ifcfg-br1` with the following content:

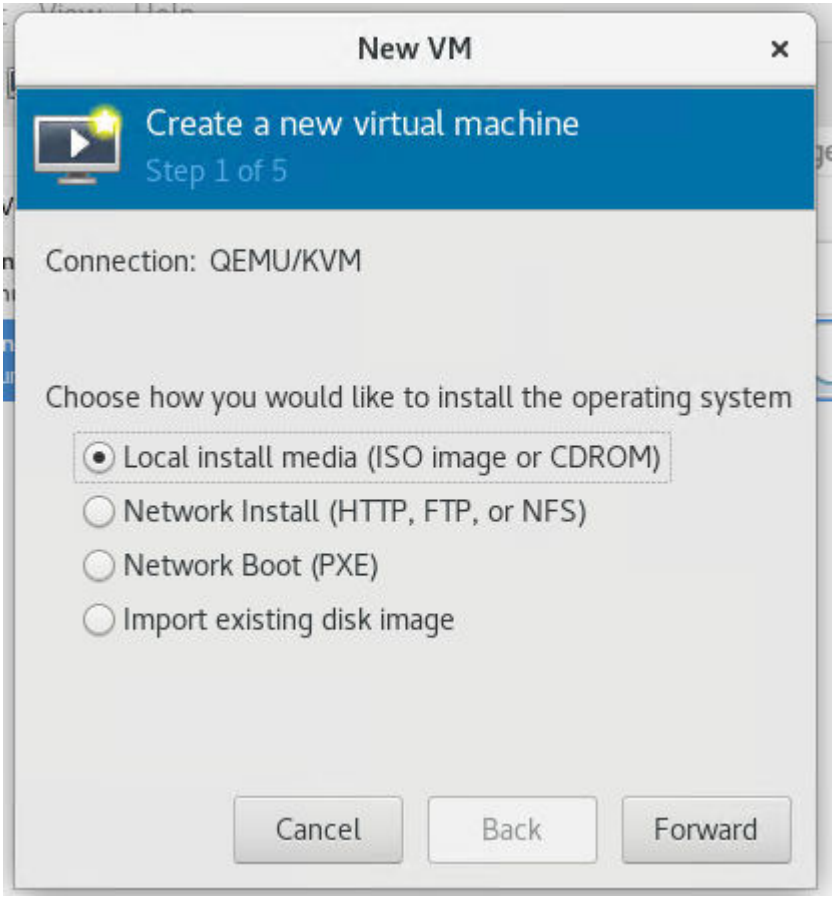
```
DEVICE=br1
BOOTPROTO=static
ONBOOT=yes
TYPE=Bridge
```

a. Restart the network service.

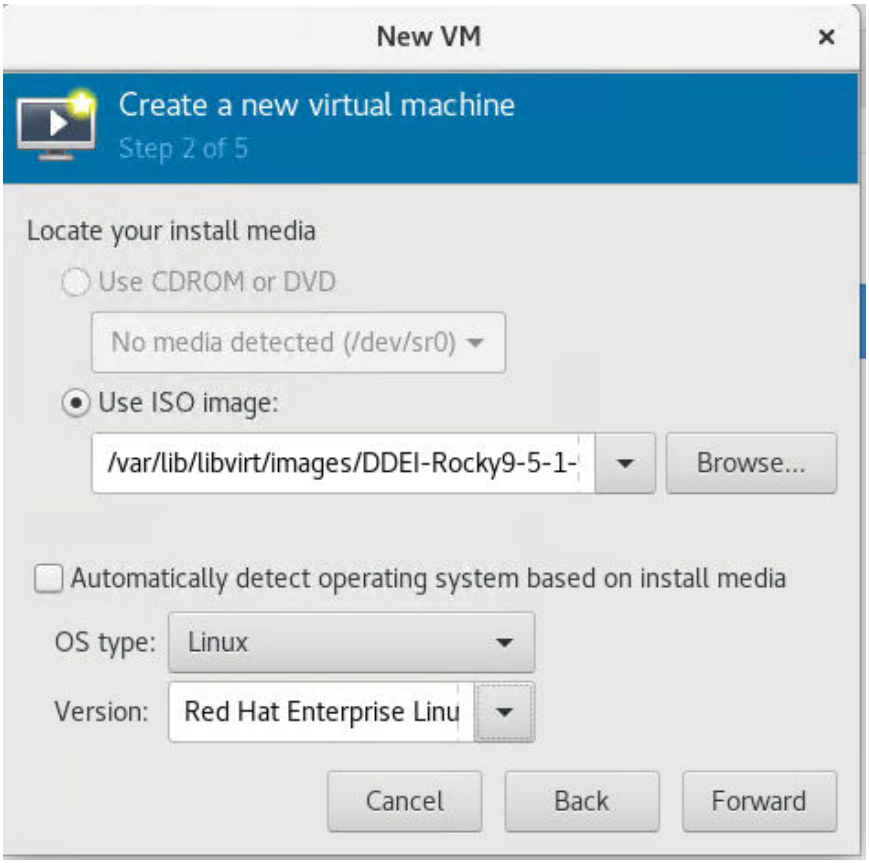
2. Open Virtual Host Manager and click **File** > **New Virtual Machine**.



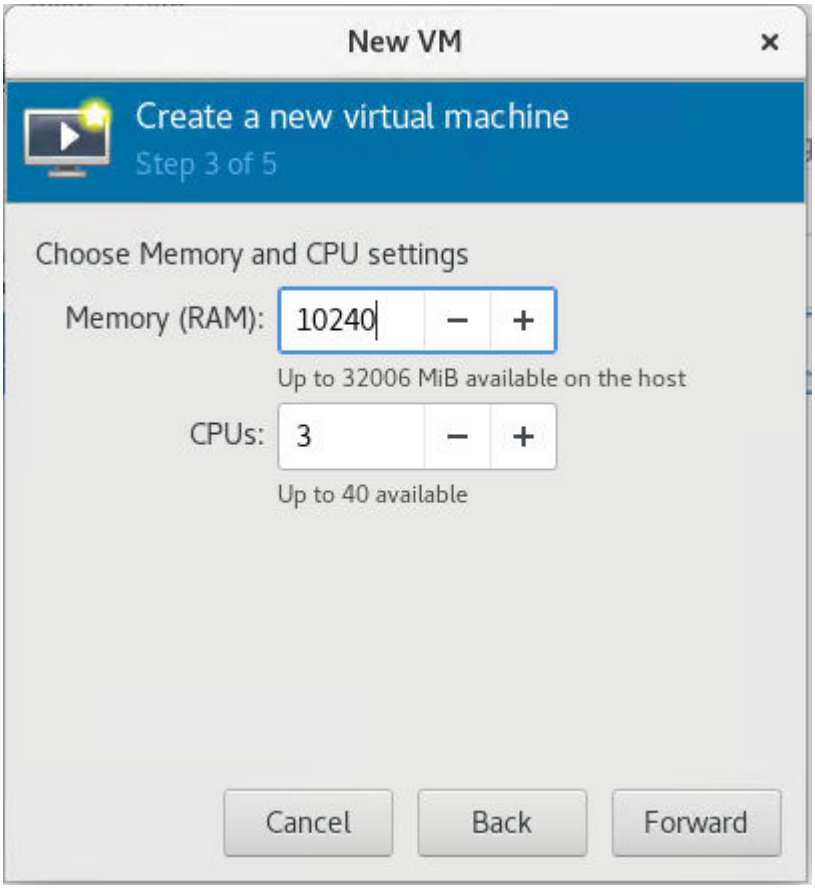
3. On the New VM screen, select **Local install media (ISO image or CDROM)** and click **Forward**.



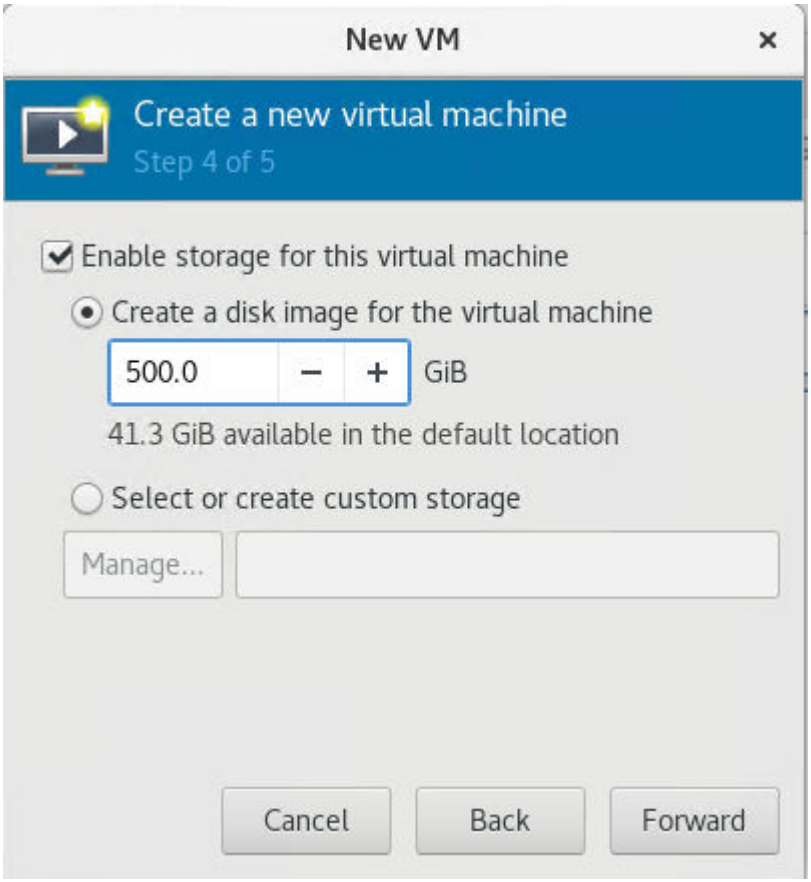
4. Select **Use ISO image** and click **Browse** to select the Deep Discovery Email Inspector installation ISO image; then, click **Forward**.



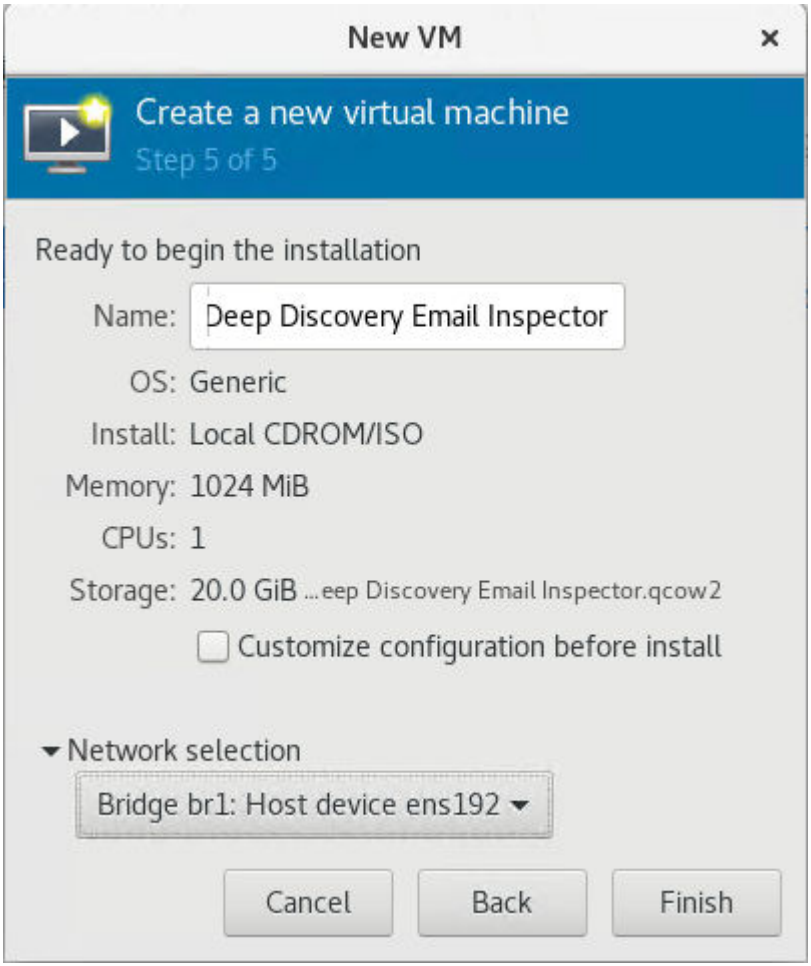
5. Configure the memory and CPU resource settings for the virtual machine and click **Forward**.



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



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**.



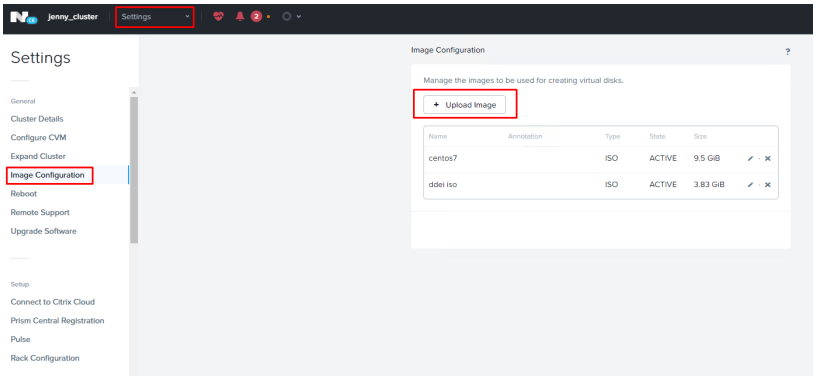
Creating a Virtual Machine on Nutanix AHV

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

Procedure

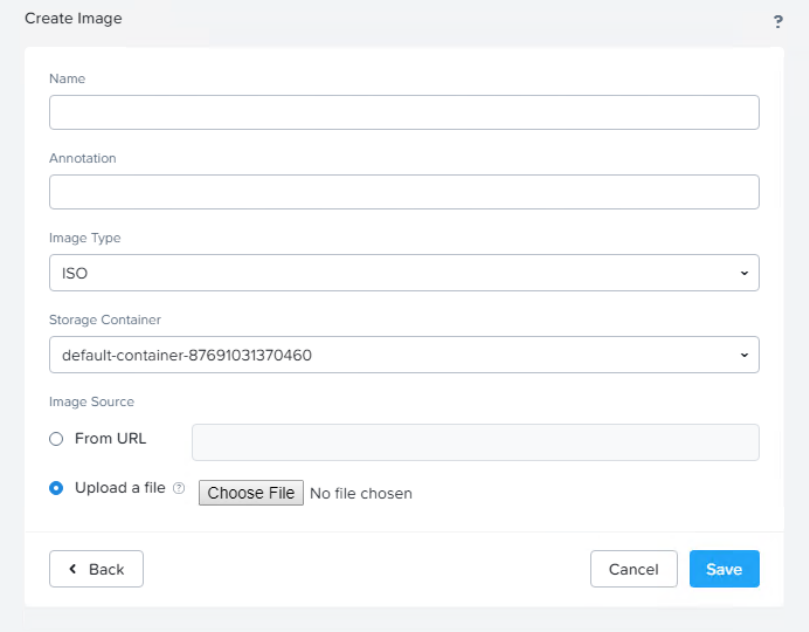
1. Access the Nutanix Prism Element web console to upload the Deep Discovery Email Inspector installation ISO image. Do the following:

   a. On the **Settings** dashboard, select **Image Configuration** and click **Upload Image**.



   The **Create Image** screen appears.

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



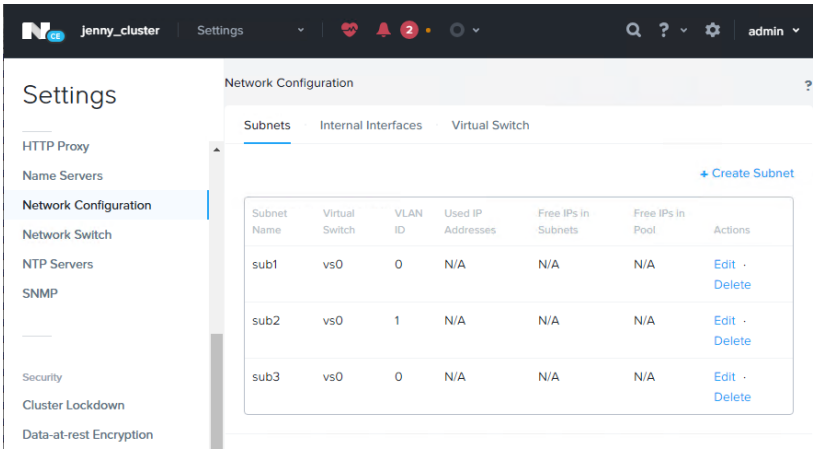
c. Select **ISO** from the **Image Type** drop-down list.

d. Select **Upload a file** and click **Choose File** to select the Deep Discovery Email Inspector installation ISO image.

e. Click **Save**.

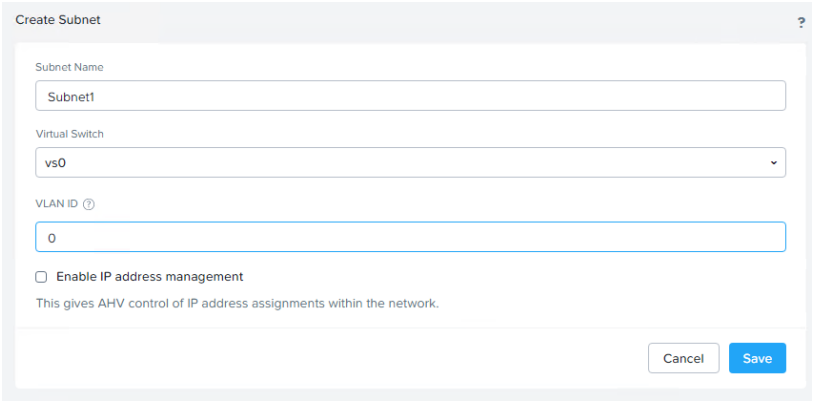
2. Create a new subnet. Do the following:

a. On the **Settings** dashboard, select **Network Configuration** and click **Subnets**.

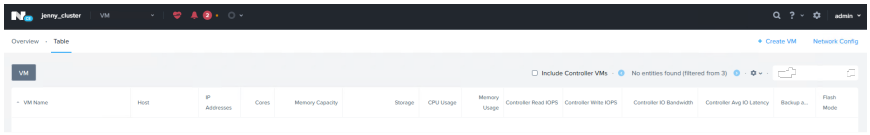


b. Click **Create Subnet**.

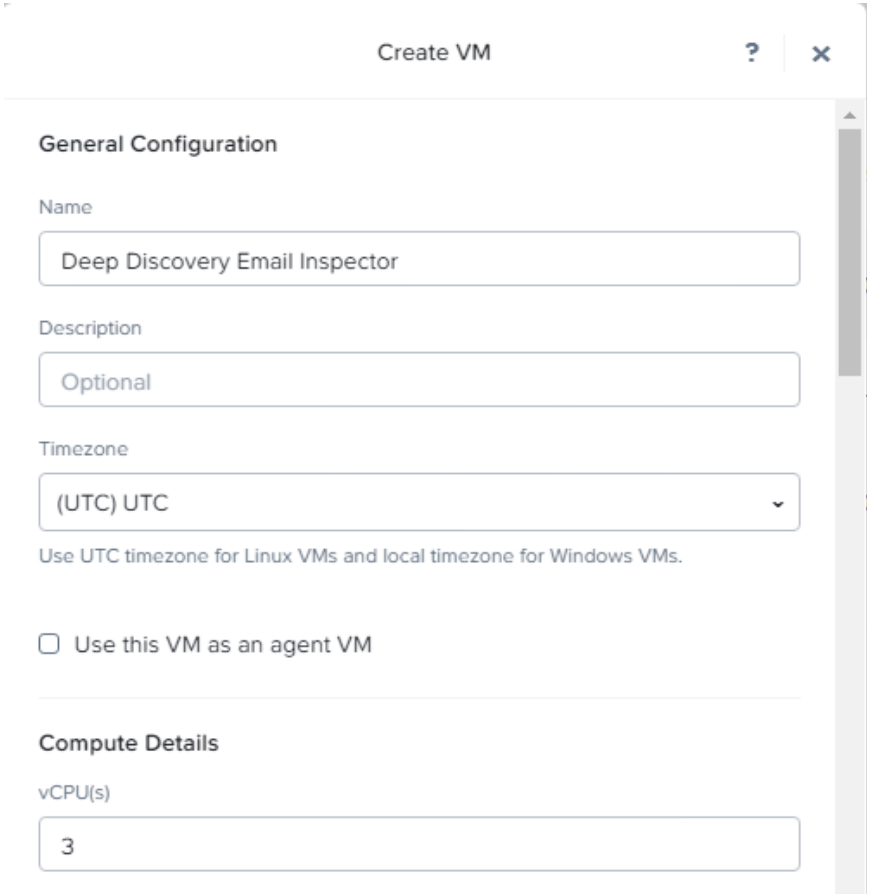
c. On the **Create Subnet** screen, type a descriptive name and type "0" for the VLAN ID; then, click **Save**.



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



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



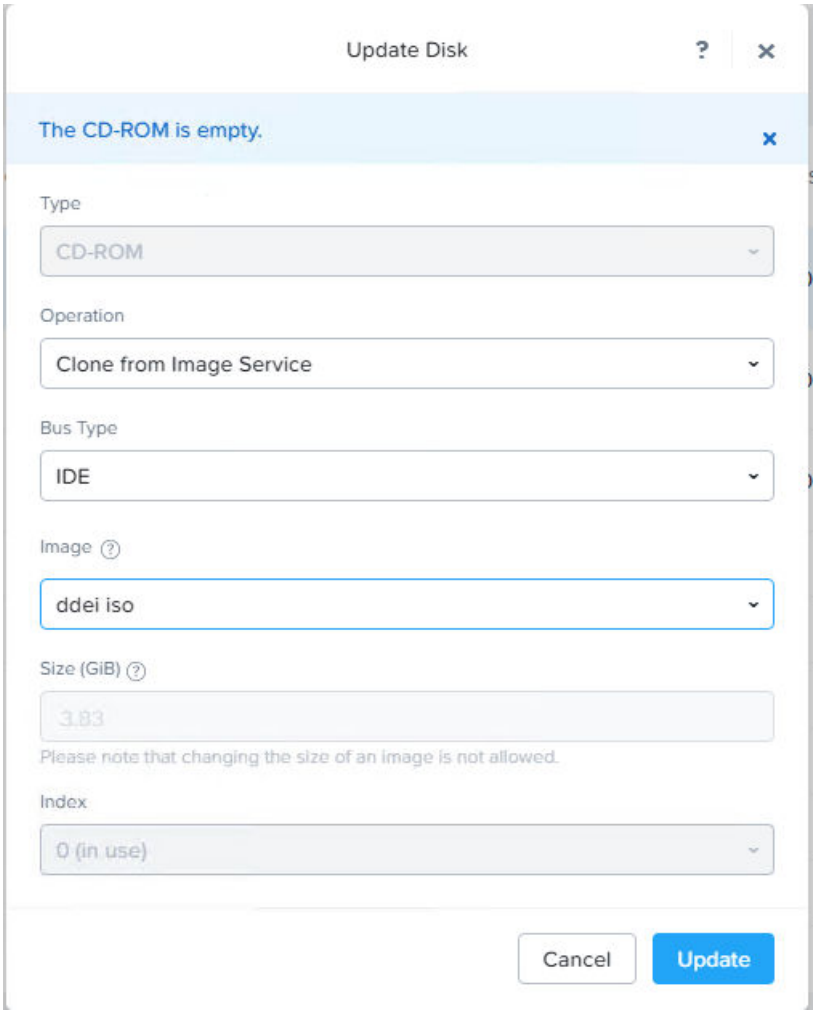
a. Type a descriptive name (for example, "Deep Discovery Email Inspector").

b. Allocate 3 or more vCPUs for the virtual machine.

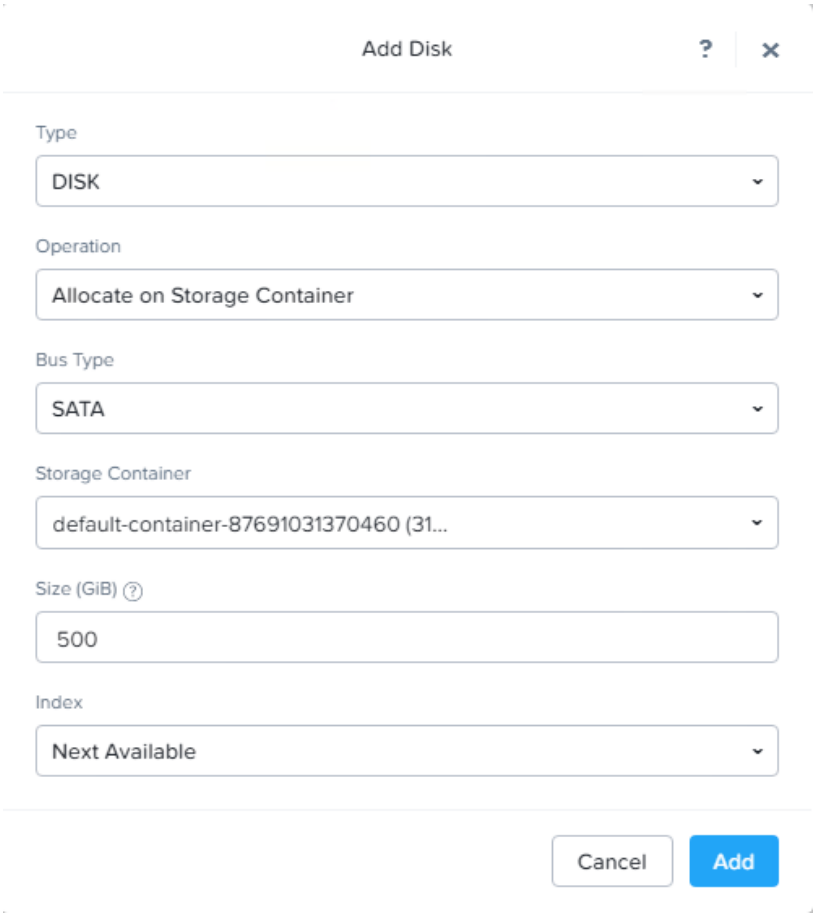
c. Allocate 10G or more memory for the virtual machine.

d. Under **Disk**, click the edit button to update the CD-ROM settings.

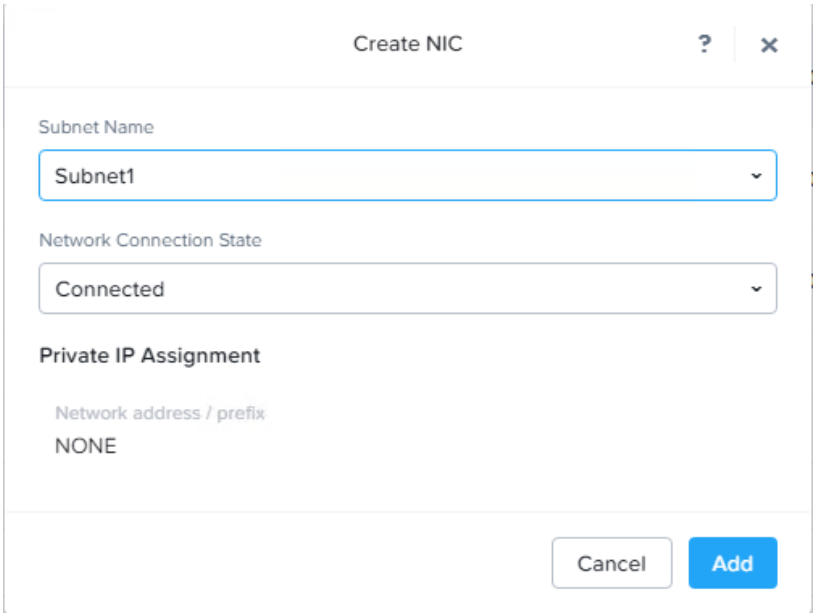
e. On the **Update Disk** screen, select the **Clone from Image Service** operation and select an image; then, click **Update**.



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



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



h. Click **Save**.

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.

Chapter 7

Technical Support

Learn about the following topics:

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

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

Contacting Trend Micro

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

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A. ※ ※
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	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

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

O

P

R

S

T

U

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

www.trendmicro.com

Item Code: APEM59195/210115