

Trend Micro™ Deep Discovery Inspector 6.7 Service Pack 1

Installation and Deployment Guide

Breakthrough Protection Against APTs and Targeted Attacks

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

https://docs.trendmicro.com

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

Copyright © 2024. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM69898/240430

Release Date: May 2024

Protected by U.S. Patent No.: 8595840; 8925074; 7707635; 8505094

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

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

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

Evaluate this documentation on the following site:

https://www.trendmicro.com/download/documentation/rating.asp

Privacy and Personal Data Collection Disclosure

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

The following link outlines the types of data that Deep Discovery 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

Part I: Introduction

Chapter 1: Introduction

About Deep Discovery Inspector	1-2
What's new	1-2
Features and benefits	1-2
Threat management capabilities APT Attack Sequence	
Host Severity	1-5
Advanced threat scan engine Virtual analyzer	

Part II: Hardware appliance installation and deployment

Chapter 2: About your system

Package contents	. 2-2
The Deep Discovery Inspector appliance	. 2-3
Front panel	2-4
Front panel - 530/1300 appliance	. 2-4
Front panel - 4300/9300 appliance	2-5
Back panel	2-5
Back panel - 530/1300 appliance	. 2-6
Back panel - 4300/9300 appliance	2-7
Network cards	2-9
Port order	2-9
Port order - 530/1300 appliance	. 2-9
Port order - 4300/9300 appliance	2-10

NIC indicators	2-12
NIC indicators - 530/1300	2-12
NIC indicators - 4300/9300	2-14
Data port indicators - 4300/9300 1 gbps	2-15
Data NIC indicators - 4300/9300 10/25 gbps	2-17
Power supply indicators	2-18
Setting up the hardware	2-19
Product specifications	2-20
Product specifications - 530/1300 appliance	2-21
Product specifications - 4300/9300 appliance	2-21

Chapter 3: Hardware appliance deployment

ii

Deployment overview	3-2
Hardware appliance deployment planning	3-2
Deployment scenarios	3-3
Out-of-band	
Mirroring trunk links	3-5
Multiple port monitoring	3-6
Network tap monitoring	3-6
Proxy monitoring	3-7
Redundant networks	3-9
Remote port or VLAN mirroring	3-9
Single port monitoring	3-10
VLAN-based port monitoring	3-12
VMware port mirroring	3-12
Inline	3-12
Transparent bridge	. 3-12
Hardware appliance installation requirements	. 3-14
Hardware appliance system requirements	3-15
Hardware appliance requirements	
Preconfiguration console requirements	
Management console requirements	
Virtual analyzer image operating system requirem	

Chapter 4: Installation on a hardware appliance

Configuring options 4-2
Setting JavaScript options for Google Chrome
Deep Discovery Inspector hardware appliance installation 4-3
Installing Deep Discovery Inspector on hardware appliances with an optical drive 4-3
Installing Deep Discovery Inspector on hardware appliances without an optical drive
Restoring to factory mode 4-15

Chapter 5: Port mirroring on a VMware virtual distributed switch

Creating a VMware vSphere distributed switch (VDS) 5-2
Deep discovery inspector hardware appliance with a VDS 5-5
Hardware appliance - configuring mirrored traffic monitoring from a VDS with encapsulated remote mirroring
Hardware appliance - configuring mirrored traffic monitoring from a VDS with remote mirroring5-9

Part III: Virtual appliance installation and deployment

Chapter 6: Virtual appliance deployment

Deployment overview	6-2
Virtual appliance deployment planning	6-2
Deployment scenarios VMware port mirroring	
Virtual appliance installation requirements	6-4
Virtual appliance system requirements Virtual host appliance requirements	

iii

Management console red	quirements	6-	6
------------------------	------------	----	---

Chapter 7: Create a new virtual appliance

-2
-2
-2
-7
13
14
14
36
37
39

Chapter 8: Installation on a virtual appliance

iv

Configuring options	8-2
Setting JavaScript options for Google Chrome	8-2
Setting JavaScript options for Mozilla Firefox	8-2
Setting options for virtual appliance in ESXi	8-3
Deep Discovery Inspector virtual appliance installation	8-4

Chapter 9: Port mirroring on a VMware virtual distributed switch

Creating a VMware vSphere distributed switch (VDS)	9-2
Deep discovery inspector virtual appliance with a VDS	9-5
Requirements for virtual appliances with a VDS Virtual appliance - monitoring mirrored external network	
traffic using a VDS	9-7
Virtual appliance - configuring mirrored external network traffic monitoring with encapsulated remote	
mirroring	

Virtual appliance - configuring mirrored external
network traffic monitoring with remote mirroring 9-10
Virtual appliance - monitoring mirrored VM traffic from a
VDS
Virtual appliance - monitoring mirrored traffic from
different ESXi hosts 9-14
Virtual appliance - configuring mirrored VM traffic
monitoring with encapsulated remote mirroring
9-15
Virtual appliance - configuring mirrored VM traffic
monitoring with remote mirroring
Virtual appliance - monitoring mirrored traffic from the
same ESXi host 9-26
Virtual appliance - configuring distributed port
mirroring on a VDS 9-27

Part IV: Post-installation tasks

Chapter 10: Preconfiguration

10-2
10-2 VGA port
10-3 serial
10-3
10-4
10-5 10-6 10-8

Chapter 11: System tasks

System tasks overview	11-2
Performing a diagnostic test	11-2
Performing a ping test	11-3
Restarting Deep Discovery Inspector	11-4

Changing the root password	11-4
Logging off	11-5
Configuring manual traffic bypass	11-5

Chapter 12: Troubleshoot

Frequently asked questions (FAQs)	. 12-2
FAQs - appliance rescue	. 12-2
FAQs - configuration	
FAQs - detections	12-3
FAQs - installation	
FAQs - upgrade	12-4
FAQs - virtual analyzer image	. 12-4
Troubleshooting	12-5
Slow management console response	. 12-5
Detections	
No detections on all detections screen	. 12-6
"unregistered service" server displays in all detectio	ns
query	12-7
Unknown IP addresses display on a screen	. 12-7
Known safe objects flagged as malicious	. 12-7
"database is corrupt" alert displays	. 12-8
Virtual analyzer	. 12-8
Cannot upload OVA	. 12-8
No virtual analyzer response to file submissions	
Virtual analyzer images	
The installation media does not start	
"found new hardware" wizard	12-10
An image displays a blue screen	12-10
Cannot connect to network services	12-11
Diagnostics	12-11
Inline deployment and TLS inspection	12-12
Network connectivity issue	
TLS connection issue	12-14

Part V: Technical support

vi

vii

Chapter 13: Troubleshooting resources
Using the support portal 13-2
Threat encyclopedia13-2
Chapter 14: Contacting Trend Micro
Speeding up the support call14-3
Chapter 15: Sending suspicious content to Trend Micro
Email Reputation Services 15-2
File Reputation Services 15-2
Web Reputation Services 15-2
Chapter 16: Other resources
Download center 16-2
Documentation feedback 16-2
Appendix A: Ports used by the appliance
Index







Preface

Preface

Learn more about the following topics:

- Documentation on page 2
- Audience on page 3
- Document Conventions on page 3

Documentation

The documentation set for Deep Discovery Inspector includes the following:

DOCUMENT	DESCRIPTION
Administrator's Guide	The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Inspector, and explanations on Deep Discovery Inspector concepts and features.
AWS Deployment Guide	The AWS Deployment Guide contains information about requirements and procedures for planning deployment, deploying, and troubleshooting Deep Discovery Inspector deployment on AWS.
Inline (LAN bypass) Network Interface Card Installation Guide	The Inline (LAN bypass) Network Interface Card Installation Guide contains information about requirements and procedures for installing an additional bypass network interface card on supported Deep Discovery Inspector appliances.
Installation and Deployment Guide	The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Inspector, and using the Preconfiguration Console to set initial configurations and perform system tasks.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Inspector.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery 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.

DOCUMENT	DESCRIPTION
Online Help	Web-based documentation that is accessible from the Deep Discovery Inspector management console.
	The Online Help contains explanations of Deep Discovery Inspector components and features, as well as procedures needed to configure Deep Discovery Inspector.
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: <u>https://success.trendmicro.com</u>

View and download product documentation from the Trend Micro Online Help Center:

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

Audience

The Deep Discovery 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
- Database management
- · Antivirus and content security protection

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
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
Г р Тір	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options



Part I Introduction





1-1

Chapter 1

Introduction

Learn about product features, capabilities, and security technology in the following topics:

- About Deep Discovery Inspector on page 1-2
- Features and benefits on page 1-2
- Threat management capabilities on page 1-3
- APT Attack Sequence on page 1-4
- Host Severity on page 1-5
- Advanced threat scan engine on page 1-7
- Virtual analyzer on page 1-8

About Deep Discovery Inspector

Deep Discovery Inspector is a third-generation threat management solution designed and architected to deliver breakthrough targeted attack and advanced threat visibility, insight, and control. Deep Discovery Inspector provides IT administrators with critical security information, alerts, and reports.

Trend Micro developed Deep Discovery Inspector to meet the requirements of G1000 organizations and government around the world. Deep Discovery Inspector integrates global intelligence and scanning technology to catch traditional signature-based threats and more sophisticated threats requiring heuristic analysis.

What's new

The following table outlines the new features in Deep Discovery Inspector 6.7 SP1.

FEATURE	DESCRIPTION
Extend the network ports of Deep Discovery Inspector 530/1300	You can now extend the network ports of your Deep Discovery Inspector 530/1300 appliances by adding any of the supported network interface cards: • Dual_Port_1GbE_Copper
Suspicious Object List Synchronization with Trend Vision One without Service Gateway	 Dual_Port_1GbE_Fiber Deep Discovery Inspector can now synchronize suspicious objects and exceptions with Trend Vision One without using a service gateway.

Features and benefits

Deep Discovery Inspector offers sophisticated detection capabilities using multiple advanced detection engines to present detailed information about

1-2

custom and signature-based threats passing through various network protocols. Deep Discovery Inspector detects targeted attacks and advanced threats, and helps remediate targeted attacks with automated processes.

Deep Discovery Inspector includes the following features:

- Threat management capabilities on page 1-3
- APT Attack Sequence on page 1-4
- Host Severity on page 1-5
- Advanced threat scan engine on page 1-7
- Virtual analyzer on page 1-8

Threat management capabilities

Deep Discovery Inspector detects and identifies evasive threats in realtime, and provides in-depth analysis and actionable intelligence needed to discover, prevent, and contain attacks against corporate data.

TABLE 1-1. Threat Management Capabilities

CAPABILITY	DESCRIPTION
Expanded APT and targeted attack detection	Deep Discovery Inspector detection engines deliver expanded APT and targeted attack detection including custom sandbox analysis. New discovery and correlation rules detect malicious content, communication, and behavior across every stage of an attack sequence.
Visibility, analysis, and action	Using an intuitive multi-level format, the Deep Discovery Inspector management console provides real-time threat visibility and analysis. This allows security professionals to focus on the real risks, perform forensic analysis, and rapidly implement containment and remediation procedures.
High capacity platforms	Deep Discovery Inspector features a high-performance architecture that meets the demanding and diverse capacity requirements of large organizations.
	Deep Discovery Inspector features are useful for a company of any size, and are vital to larger organizations needing to reduce the risk of targeted attacks.

APT Attack Sequence

Targeted attacks and advanced persistent threats (APTs) are organized, focused efforts that are custom-created to penetrate enterprises and government agencies for access to internal systems, data, and other assets. Each attack is customized to its target, but follows a consistent life cycle to infiltrate and operate inside an organization.

In targeted attacks, the APT life cycle follows a continuous process of six key phases.

PHASE	DESCRIPTION
Intelligence Gathering	Identify and research target individuals using public sources (for example, social media websites) and prepare a customized attack
Point of Entry	An initial compromise typically from zero-day malware delivered via social engineering (email/IM or drive-by download)
	A backdoor is created and the network can now be infiltrated. Alternatively, a website exploitation or direct network hack may be employed.
Command & Control (C&C)	Communications used throughout an attack to instruct and control the malware used
Communication	C&C communication allows the attacker to exploit compromised machines, move laterally within the network, and exfiltrate data.
Lateral Movement	An attack that compromises additional machines
	Once inside the network, an attacker can harvest credentials, escalate privilege levels, and maintain persistent control beyond the initial target.
Asset/Data Discovery	Several techniques (for example, port scanning) used to identify noteworthy servers and services that house data of interest
Data Exfiltration	Unauthorized data transmission to external locations
	Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed, and often encrypted for transmission to external locations under an attacker's control.

TABLE 1-2. APT Attack Sequence

Deep Discovery Inspector is purpose-built for detecting APT and targeted attacks. It identifies malicious content, communications, and behavior that may indicate advanced malware or attacker activity across every stage of the attack sequence.

Host Severity

In Deep Discovery Inspector, host severity is the impact on a host as determined from aggregated detections by Trend Micro products and services.

Investigating beyond event security, the host severity numerical scale exposes the most vulnerable hosts and allows you to prioritize and quickly respond.

Host severity is based on the aggregation and correlation of the severity of the events that affect a host. If several events affect a host and have no detected connection, the host severity will be based on the highest event severity of those events. However, if the events have a detected correlation, the host severity level will increase accordingly.

For example: Of five events affecting a host, the highest risk level is moderate. If the events have no correlation, the host severity level will be based on the moderate risk level of that event. However, if the events are correlated, then the host severity level will increase based on the detected correlation.

The host severity scale consolidates threat information from multiple detection technologies and simplifies the interpretation of overall severity. You can prioritize your responses based on this information and your related threat response policies.

CATEGORY	LEVEL	

TABLE 1-3. Host Severity Scale

CATEGORY	LEVEL	DESCRIPTION
Critical	10	Host shows evidence of compromise including but not limited to the following:
Host exhibits behavior that definitely indicates host is		Data exfiltration
compromised		Multiple compromised hosts/servers

CATEGORY	LEVEL	DESCRIPTION
	9	Host exhibits an indication of compromise from APTs including but not limited to the following:
		 Connection to an IP address associated with a known APT
		 Access to a URL associated with a known APT
		 A downloaded file associated with a known APT
		Evidence of lateral movement
	8	Host may exhibit the following:
		 A high severity network event
		 Connection to a C&C Server detected by Web Reputation Services
		 A downloaded file rated as high risk by Virtual Analyzer
Major	7	Host may exhibit the following:
Host is targeted by a known malicious behavior or attack and exhibits behavior that likely indicates host is compromised		 Inbound malware downloads; no evidence of user infection
		An inbound Exploit detection
	6	Host may exhibit the following:
		 Connection to a dangerous site detected by Web Reputation Services
	5	Host may exhibit the following:
		 A downloaded medium- or low-risk potentially malicious file with no evidence of user infection
	4	Host may exhibit the following:
		A medium severity network event
		 A downloaded file rated as medium risk by Virtual Analyzer

1-6

CATEGORY	LEVEL	DESCRIPTION
Minor	3	Host may exhibit the following:
Host exhibits anomalous or suspicious behavior that may		 Repeated unsuccessful logon attempts or abnormal patterns of usage
be benign or indicate a threat		 A downloaded or propagated packed executable or suspicious file
		 Evidence of running IRC, TOR, or outbound tunneling software
	2	Host may exhibit the following:
		A low severity network event
		 Evidence of receiving an email message that contains a dangerous URL
		 A downloaded file rated as low risk by Virtual Analyzer
Trivial	1	Host may exhibit the following:
Host exhibits normal		An informational severity network event
behavior that may be benign or indicate a threat in future identification of malicious activities		 Connection to a site rated as untested or to a new domain detected by Web Reputation Services
		 Evidence of a running disruptive application such as P2P

Advanced threat scan engine

Advanced Threat Scan Engine uses a combination of signature file-based scanning and heuristic rule-based scanning to detect and document exploits and other threats used in targeted attacks.

Major features include the following:

- · Detection of zero-day threats
- Detection of embedded exploit code
- Detection rules for known vulnerabilities

• Enhanced parsers for handling file deformities

Virtual analyzer

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.

Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics in the following categories:

- · Anti-security and self-preservation
- · Autostart or other system configuration
- · Deception and social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- · Malformed, defective, or with known malware traits
- · Process, service, or memory object change
- · Rootkit, cloaking

1-8

· Suspicious network or messaging activity

During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer also generates analysis reports, suspicious object lists, PCAP files, and OpenIOC and STIX files that can be used in investigations.

Part II

Hardware appliance installation and deployment





2-1

Chapter 2

About your system

Learn about the Deep Discovery Inspector appliance in the following topics:

- Package contents on page 2-2
- The Deep Discovery Inspector appliance on page 2-3
- Setting up the hardware on page 2-19
- Product specifications on page 2-20

Package contents

Examine the Deep Discovery Inspector appliance package contents and hardware to correctly configure the appliance in your network.

The following illustration shows the items that are included in the Deep Discovery Inspector appliance package.



FIGURE 2-1. Package Contents

#	ΝΑΜΕ	DESCRIPTION
1	Slide and rail sets (2)	Secure the appliance (fixed mount) or use to secure and allow the appliance to slide in and out of a four-post rack (sliding mount).
		package is shipped. Remove the rail from the slide before mounting the appliance.

2-2

#	Nаме	DESCRIPTION
2	Trend Micro Installation DVD for Deep Discovery	The Installation DVD contains installers and the PDF documentation set, including the following:
	Inspector (1) Deep Discovery Inspector	 Trend Micro Deep Discovery Inspector Administrator's Guide
	Quick Start Card	 Trend Micro Deep Discovery Inspector Installation and Deployment Guide
		The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Inspector to your network and on performing the initial configuration.
3	Power cords (2)	Supply power to the appliance (length is 79 in/200 cm)
4	Deep Discovery Inspector (1)	The appliance

The Deep Discovery Inspector appliance

Deep Discovery Inspector 6.7 SP1 supports the following hardware appliance models. You can view the model number on the front sticker of your physical appliance.

- 520
- 530
- 1100
- 1200
- 1300
- 4100
- 4200
- 4300
- 9200
- 9300

Front panel

Front panel - 530/1300 appliance



FIGURE 2-2. Deep Discovery Inspector 530/1300 Front Panel

The following table outlines the front panel features of the 530/1300 appliance.

#	FEATURE	DESCRIPTION
1	Status LED indicators	Displays system ID, status information, and system error messages
2	Optical drive	DVD drive
3	Video connector	Connects a VGA display to the appliance
4	Power-on indicator	• Lights when the system power is on
	Power button	 Controls the power supply output to the appliance
5	USB connector	Connects USB devices (for example, keyboard or mouse) to the appliance
6	iDRAC Direct port (Micro-AB USB)	Enables you to access the iDRAC Direct (Micro-AB) features
7	Hard drives (2)	3.5-inch, hot-swappable

2-4

Front panel - 4300/9300 appliance



FIGURE 2-3. Deep Discovery Inspector 4300/9300 Front Panel

The following table outlines the front panel features of the 4300/9300 appliance.

#	FEATURE	DESCRIPTION
1	Status LED indicators	Displays system ID, status information, and system error messages
2	Front ID button/indicator	Not supported by Deep Discovery Inspector
3	Power-on button/indicator	 Lights when the system power is on Controls the power supply output to the appliance
4	USB connector	Allows you to connect USB devices to the appliance
5	Video connector	Allows you to connect a VGA display to the appliance
6	iDRAC Direct port (Micro-AB USB)	Enables you to access the iDRAC Direct (Micro-AB) features
7	Hard drives (4)	3.5-inch, hot-swappable hard drive

Back panel

Back panel - 530/1300 appliance

2-6

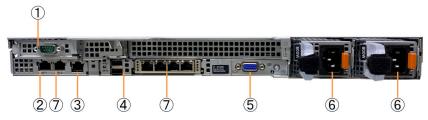


FIGURE 2-4. Deep Discovery Inspector 530/1300 Back Panel

The following table outlines the back panel features of the 530/1300 appliance.

#	FEATURE	DESCRIPTION
1	RS-232 serial connector	Connects to the serial port of a computer with an RS-232 type connection to perform preconfiguration
2	Management port	Connects to a management network for communication and interaction with other products and services
3	iDRAC port	Connects to a dedicated management port on the iDRAC card
4	USB connectors (2)	Connects USB devices (for example, keyboard or mouse) to the appliance
5	Video connector	Connects a VGA display to the appliance

#	FEATURE	DESCRIPTION
6	Power supply connectors (2)	Two 800-watt hot-plug power supply units: • Main power supply • Backup power supply
		Note "Hot-plug" refers to the ability to replace the power supply while the appliance is running. Deep Discovery Inspector automatically and safely recognizes the change without operational interruption or risk.
		Use the power cord included in the package (for details, see <i>Package contents on page 2-2</i>).
7	Data ports (5)	Five integrated 1 Gbps NIC connectors

Back panel - 4300/9300 appliance

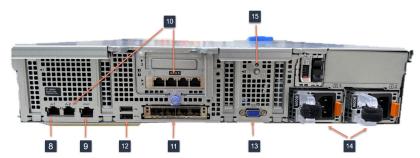


FIGURE 2-5. Deep Discovery Inspector 4300/9300 Back Panel

The following table outlines the back panel features of the 4330/9300 appliance.

#	FEATURE	DESCRIPTION
8	Management port	Connects to a management network for communication and interaction with other products and services
9	iDRAC port	Connects to a dedicated management port on an iDRAC card
10	1 Gbps data ports (5)	Five integrated 10/100/1000 Mbps Base-T NIC connectors
11	10/25 Gbps data ports (4)	Four 10/25 Gbps NIC connectors
12	USB connectors (2)	Connects USB devices (for example, keyboard or mouse) to the appliance
13	Video connector	Connects a VGA display to the appliance
14	Power supply connectors (2)	 Two 800-watt (4300) or 1100-watt (9300) hotplug power supply units (see your device labels for wattage): Main power supply Backup power supply
		Note "Hot-plug" refers to the ability to replace the power supply while the appliance is running. Deep Discovery Inspector automatically and safely recognizes the change without operational interruption or risk. Use the power cord included in the package (for details, see Package contents on page 2-2).

2-8

#	FEATURE	DESCRIPTION
15	Appliance ID button / appliance status indicator	Not supported by Deep Discovery Inspector

Network cards

Port order

Port order - 530/1300 appliance



Тір

To see information about the card slots, go to **Administration** > **System Settings** > **Network Interface** in the Deep Discovery Inspector management console.

The following table outlines the port order of the network cards in the 530/1300 appliance.

NIC	SLOT	Port order
Dedicated_Quad_Por t_1GbE_Copper	Dedicated	
Dual_Port_1GbE_Cop per_Bypass_Card	Slot 1	

NIC	SLOT	Port order
Dual_Port_10GbE_Fi ber-SR_Bypass_Card	Slot 1	
Dual_Port_1GbE_Cop per	Slot 1	
Dual_Port_1GbE_Fib er	Slot 1	

Port order - 4300/9300 appliance

To see information about the card slots, go to **Administration** > **System Settings** > **Network Interface** in the Deep Discovery Inspector management console.





Important

- Slot 1 is a RAID controller.
- Slot 5 and slot 6 are not available for use on the 4300 appliance.

The following table outlines the port order of the network cards in the 4300/9300 appliance.

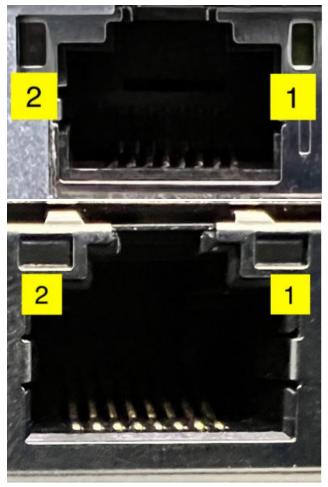
NIC	SLOT	Port order
Dedicated_Quad_Por t_10/25GbE_SFP28	• Dedicated	
Quad_Port_1GbE_Co pper	Slot 3Slot 4	4 3 2 1
	 Slot 2 Slot 5 (9300 only) Slot 6 (9300 only) 	
Dual_Port_10GbE_Fi ber-SR_Bypass_Card	Slot 2	

NIC indicators

2-12

NIC indicators - 530/1300

For out-of-band deployment, Deep Discovery Inspector 530/1300 has five user-configurable copper-based Ethernet NIC ports. All accept integrated 10/100/1000 Mbps connectors.



Each port has an indicator showing the current state of the port.

FIGURE 2-6. The two port types found in the Deep Discovery Inspector 530/1300 appliance

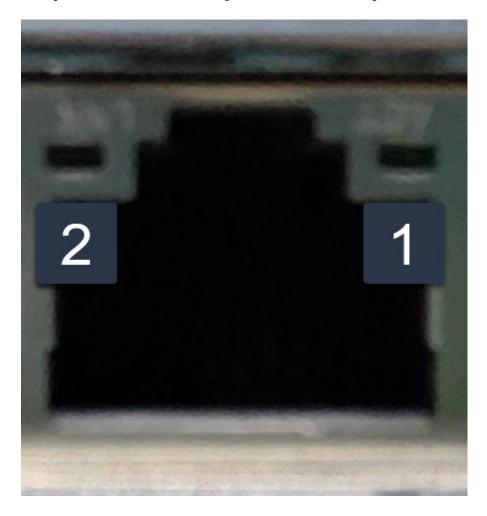
The following table describes the NIC indicators in the 530/1300 appliance.

INDICAT OR	DESCRIPTION	INDICATOR PATTERN
1	Indicates the connection status and data activity status.	 Off: No network connection. Green, flashing: Network data is being sent or received.
2	Indicates the data transmission speed.	Yellow: 10 Mbps or 100 MbpsGreen: 1000 Mbps

NIC indicators - 4300/9300



Data port indicators - 4300/9300 1 gbps Each port has an indicator showing the current state of the port.



The following table describes the 1 Gbps port indicators in the 4300/9300 appliance.

INDICAT OR	DESCRIPTION	INDICATOR PATTERN
1	Indicates the connection status and data activity status.	 Off: No network connection. Green, flashing: The port is sending or receiving data.
2	Indicates the data transmission speed.	Yellow: 10 Mbps or 100 MbpsGreen: 1000 Mbps

Data NIC indicators - 4300/9300 10/25 gbps

Each port has an indicator showing the current state of the port.



The following table describes the 10/25 Gbps NIC indicators in the 4300/9300 appliance.

INDICAT OR	DESCRIPTION	INDICATOR PATTERN
1	Indicates the connection status and data activity status.	 Off: No network connection. Green, flashing: Network data is being sent or received.
2	Indicates the data transmission speed.	Yellow: 10 GbpsGreen: 25 Gbps

Power supply indicators

The following table outlines the power supply status indicators.

INDICATOR PATTERN	DESCRIPTION
Not lit	Power is not connected
Green	A valid power source is connected to the power supply and the power supply is operational
Flashing green	When hot-adding a power supply, indicates the power supply is mismatched with the other power supply (in terms of efficiency, feature set, health status, and supported voltage)
	Replace the power supply that has the flashing indicator with a power supply that matches the capacity of the other installed power supply.

INDICATOR PATTERN	DESCRIPTION
Flashing amber	Indicates a problem with the power supply
	Important When correcting a power supply mismatch, replace only the power supply with the flashing indicator. Swapping the opposite power supply to make a matched pair can result in an error condition and an unexpected system shutdown.
	To change from a high output configuration to a low output configuration or vice versa, first power down the system.
	AC power supplies support both 220 V and 110 V input voltages. When two identical power supplies receive different input voltages, they may output different wattages and trigger a mismatch.
	If two power supplies are used, they must be of the same type and have the same maximum output power.

Setting up the hardware

Procedure

Mount the appliance in a standard 19-inch 4-post rack, or on a free-1. standing object, such as a sturdy desktop.



When mounting the appliance, leave at least two inches of clearance on all sides for proper ventilation and cooling.

Connect the appliance to a power source. 2.

Deep Discovery Inspector has two power supply units. One unit acts as the main power supply and the other as a backup.

3. Connect the monitor to the VGA port at the back panel.

See Back panel on page 2-5 for a diagram.

- 4. Connect the keyboard and mouse to the USB ports on the back panel.
- 5. Connect the management port to your network.
- **6.** Power on the appliance.

The power button is found on the front panel of the appliance, behind the bezel. See *Front panel on page 2-4* for a diagram.

A screen similar to the following appears:

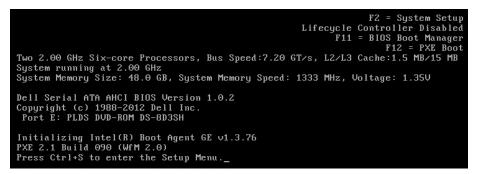


FIGURE 2-7. Power-on self-test (POST)

What to do next

If applicable, perform initial preconfiguration using the Preconfiguration Console. For details, see *Preconfiguration on page 10-1*.

Product specifications

Standard Deep Discovery Inspector appliances have the following specifications.

Contact Trend Micro if the appliance you are using does not meet these hardware specifications.

Note

Hardware vendors and specifications may vary for customers in China, Japan, and other regions.

Product specifications - 530/1300 appliance

TABLE 2-2. Deep Discovery Inspector 530/1300	

FEATURE	Specifications
Rack size	1U 19-inch standard rack
Availability	Raid 1 configuration
Storage size	2 x 2 TB 3.5-inch SATA
Connectivity	Management: 1 x 1 GB/100/10Base copper
	• Data: 5 x 1 GB/100/10Base copper
Dimensions (WxDxH)	482.0 mm (18.97 inches) x 748.79 mm (29.48 inches) x 42.8 mm (1.68 inches)
Maximum weight	18.62 kg (41.05 lb)
Operating temperature	10°C to 35°C at 10% to 80% relative humidity (RH)
Power	800W, 100-240 VAC 50/60 Hz

Product specifications - 4300/9300 appliance

TABLE 2-3. Deep Discovery Inspector 4200/9200 Appliance

FEATURE	Specifications
Rack size	2U 19-inch standard rack
Availability	Raid 10 configuration
Storage size	4 x 2 TB 3.5-inch SATA

FEATURE	Specifications
Connectivity	• Management: 1 x 1 GB/100/10Base copper
	• Data:
	4 x 10/25 GB SFP28 DAC, Optics, And AOC's
	5 x 1 GB/100/10Base copper
Dimensions (WxDxH)	482.0 mm (18.97 inches) x 685.78 mm (26.99 inches) x 86.8 mm (3.41 inches)
Maximum weight	28.82 kg (63.53 lb)
Operating temperature	10°C to 35°C at 10% to 80% relative humidity (RH)
Power	800W (4300) / 1100W (9300), 100-240 VAC 50/60 Hz



3-1

Chapter 3

Hardware appliance deployment

Learn tips, suggestions, and requirements for installing a Deep Discovery Inspector hardware appliance in the following sections.

Deployment overview

Procedure

- Plan the deployment.
 See Hardware appliance deployment planning on page 3-2.
- 2. Review the installation requirements.

See Hardware appliance installation requirements on page 3-14.

- **3.** Review the system requirements. See *Hardware appliance system requirements on page 3-15*.
- Install Deep Discovery Inspector.
 See Installation on a hardware appliance on page 4-1.
- 5. Preconfigure Deep Discovery Inspector.

See Preconfiguration on page 10-1.

Hardware appliance deployment planning

Plan how to best deploy Deep Discovery Inspector by doing the following:

- Determine the segments of your network that need protection.
- Plan for network traffic, considering the location of appliances critical to your operations such as email, web, and application servers.
- Determine both the number of appliances needed to meet your security needs and their locations on the network
- Conduct a pilot deployment on a test segment of your network.
- Redefine your deployment strategy based on the results of the pilot deployment.
- Use the following examples to plan a customized Deep Discovery Inspector deployment.

Deployment scenarios

Deep Discovery Inspector can be deployed as a hardware appliance or as a virtual appliance.

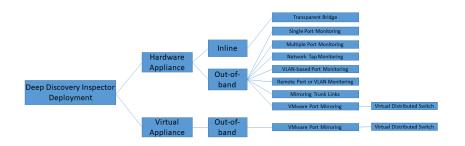
- Hardware appliance: Deep Discovery Inspector can be deployed either inline or out-of-band.
 - Inline: Deep Discovery Inspector acts as a transparent bridge and can inspect decrypted TLS traffic. When deployed inline, only traffic flowing through the inline ports is inspected.



Installing an additional inline (LAN bypass) network interface card is needed for inline deployment. For installation instructions and compatible Deep Discovery Inspector appliance models, refer to the *Inline (LAN Bypass) Network Interface Card Installation Guide*.

- Out-of-band: Deep Discovery Inspector monitors network traffic by connecting to the mirror port on a switch for minimal to no network interruption. When deployed out-of-band, only traffic mirrored to the data ports is inspected.
- Virtual appliance: Deep Discovery Inspector can only be deployed out-of-band. Deep Discovery Inspector monitors network traffic by connecting to the mirror port on a switch for minimal to no network interruption.

The figure below provides a high-level overview of supported deployments.



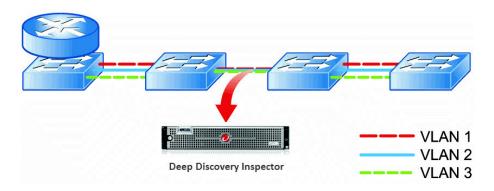
Out-of-band

3-4

When deployed out-of-band, Deep Discovery Inspector monitors network traffic by connecting to the mirror port on a switch for minimal to no network interruption.

Mirroring trunk links

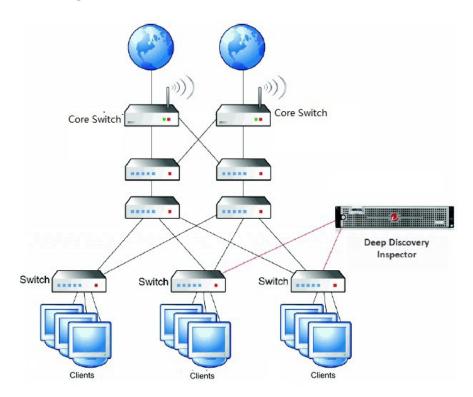
When multiple VLANs encapsulate the same physical link, mirror the source port from a trunk link. Make sure that the switch mirrors the correct VLAN tag to Deep Discovery Inspector for both directions.





Multiple port monitoring

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



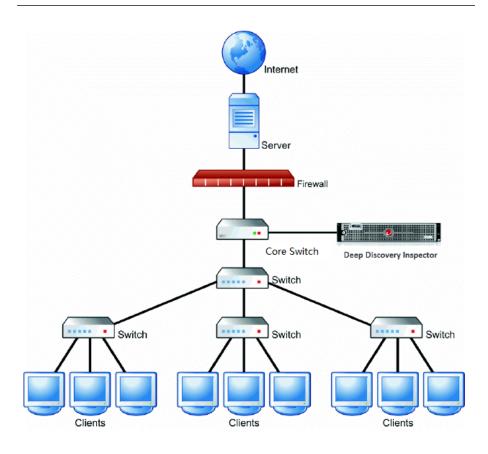
Network tap monitoring

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



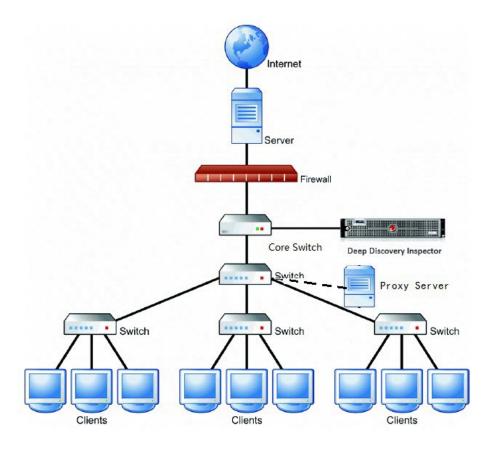
note 📍

If using network taps, make sure that they copy DHCP traffic to Deep Discovery Inspector instead of filtering DHCP traffic.



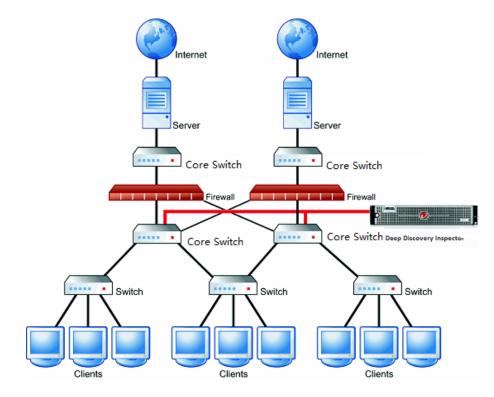
Proxy monitoring

When configuring Deep Discovery Inspector in proxy environments outside the proxy server, enable XFF on the proxy server. To avoid false alarms when configuring Deep Discovery Inspector in proxy environments inside or outside the proxy server, add HTTP Proxy as a registered service on Deep Discovery Inspector.



Redundant networks

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



Remote port or VLAN mirroring

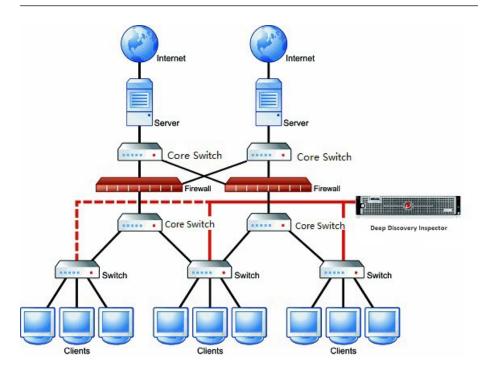
Use remote mirroring in the following conditions:

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



Note

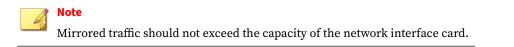
In this diagram, the dotted line displays the remote mirror, and the solid line displays the direct mirror.

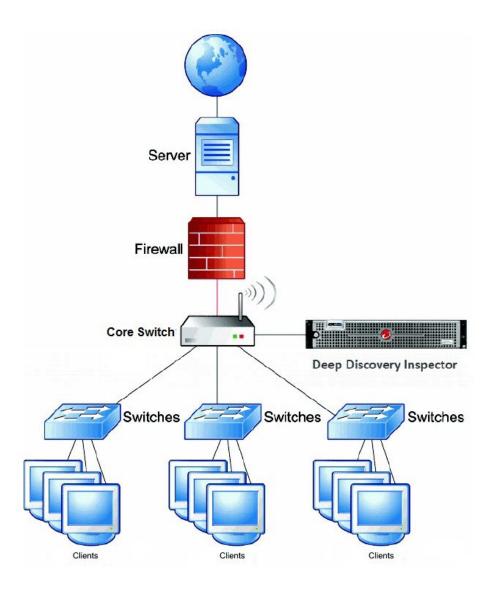


Single port monitoring

The Deep Discovery Inspector data port connects to the mirror port of the core switch, which mirrors the traffic through the port to the firewall.

(Optional) Configure the mirror port to mirror inbound/outbound traffic from single or multiple source ports.





VLAN-based port monitoring

VLAN-based port mirroring allows users to choose to monitor traffic on all ports belonging to a particular VLAN. In this scenario, connect Deep Discovery Inspector to a switch if the mirror configuration is VLAN-based.

VMware port mirroring

Use VMware port mirroring when traffic passes through a virtual distributed switch.

For more details, see *Port mirroring on a VMware virtual distributed switch on* page 5-1.

Inline

When deployed inline, Deep Discovery Inspector acts as a transparent bridge and can inspect decrypted TLS traffic.



Note

Installing an additional inline (LAN bypass) network interface card is needed for inline deployment. For installation instructions and compatible Deep Discovery Inspector appliance models, refer to the *Inline (LAN Bypass) Network Interface Card Installation Guide*.

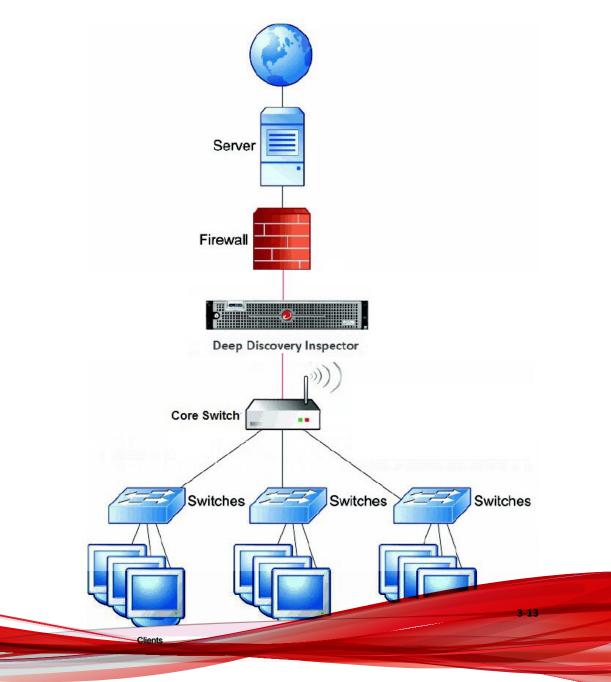
Traffic cannot be blocked by Deep Discovery Inspector. When Deep Discovery Inspector is deployed inline, traffic is only inspected or not inspected.

Transparent bridge

Transparent bridge deployment is suitable when you want to use Deep Discovery Inspector as an inline device. Transparent bridge deployment is required for TLS traffic inspection.

When deployed as a transparent bridge, Deep Discovery Inspector acts as a layer 2 bridge between network devices and is transparent on the network

and you do not need to reconfigure your network as you need only place the appliance in the network path that you want to monitor.



Hardware appliance installation requirements

Ensure the following before installing Deep Discovery Inspector.

REQUIREMENT	DESCRIPTION
Match port speeds	The destination port speed should be the same as the source port speed to ensure equal port mirroring. If the destination port is unable to handle the faster speed of the source port, the destination port may drop some data.
	For Deep Discovery Inspector 530/1300, the speed of inline ports is downgraded if not matched.
	For Deep Discovery Inspector 4200/9200, the inline ports are disabled if not matched.
Configure Virtual Analyzer data ports	When enabling an internal Virtual Analyzer, select one of the following network options and make sure the data ports are configured as follows:
	No Network
	Virtual Analyzer does not exchange data with the Internet.
	Custom Network
	Virtual Analyzer uses an additional specified data port to exchange data with the Internet.
	Management Network
	Virtual Analyzer uses a management port to exchange data with the Internet.
	For details, see Internal Virtual Analyzer in the Deep Discovery Inspector Administrator's Guide.

REQUIREMENT	DESCRIPTION
Monitor all data	Deep Discovery Inspector monitors all inbound and outbound network traffic.
	Note For better performance when installing Deep Discovery Inspector, Trend Micro recommends using a plug-in NIC rather than an onboard NIC as a data port.
	Note To ensure Deep Discovery Inspector captures traffic from both directions, configure the mirror port, and make sure that traffic in both directions is mirrored to the port.

Hardware appliance system requirements

Deep Discovery Inspector requires the following:

- Hardware appliance requirements on page 3-15
- Preconfiguration console requirements on page 3-16
- Management console requirements on page 3-16
- Virtual analyzer image operating system requirements on page 3-17

Hardware appliance requirements

Trend Micro provides the Deep Discovery Inspector appliance hardware. No other hardware is supported.

Installing an additional inline (LAN bypass) network interface card is needed for inline deployment. For installation instructions and compatible Deep Discovery Inspector appliance models, refer to the *Inline (LAN Bypass) Network Interface Card Installation Guide*.

Preconfiguration console requirements

The Deep Discovery Inspector Preconfiguration Console is a terminal communications program used to configure the network and system settings that are required to access the Deep Discovery Inspector management console.

For details, see Preconfiguration console on page 10-2

Access to the Preconfiguration Console requires the following:

- VGA connections:
 - Monitor with a VGA port
 - USB keyboard
 - VGA cable
- Serial connections:
 - Computer with a serial port
 - RS-232 serial cable
 - Serial communication application (HyperTerminal)

Management console requirements

Deep Discovery Inspector provides a built-in online management console for viewing system status, configuring and viewing threat detections and logs, running reports, administering Deep Discovery Inspector, updating components, and obtaining help.

For details, see *Management Console* in the *Deep Discovery Inspector Administrator's Guide*.

The Deep Discovery Inspector management console supports the following web browsers:

- Google[™] Chrome[™]
- Mozilla[™] FireFox[™]

• Microsoft[™] Edge

Recommended resolution rate: 1280x800

Virtual analyzer image operating system requirements

Windows operating systems and other Microsoft products are available separately from Microsoft and Microsoft channel partners.



Important

Trend Micro does not provide any Microsoft Windows operating systems or Microsoft Office products required for installation on Virtual Analyzer images or sandbox instances you create in Deep Discovery Inspector. You must provide the operating system and Microsoft Office installation media and appropriate licensing rights necessary for you to create any sandboxes.



Chapter 4

Installation on a hardware appliance

Learn the steps for installing Deep Discovery Inspector as a hardware appliance in the following sections.



Configuring options

Set the following options to enable Deep Discovery Inspector management console navigation.

- Setting JavaScript options for Google Chrome on page 4-2
- Setting JavaScript options for Mozilla Firefox on page 4-2

Setting JavaScript options for Google Chrome

Procedure

- 1. On the browser, go to **Settings**.
- 2. Click Show advanced settings....
- 3. Under Privacy, click Content settings....
- 4. Under JavaScript, click Allow all sites to run JavaScript (recommended).
- 5. Click Done.

Setting JavaScript options for Mozilla Firefox

Procedure

- 1. For Firefox versions lower than 23, do the following.
 - **a.** On the browser, go to the **Options** > **Content** tab.
 - **b.** Verify that **Enable JavaScript** is selected.
 - c. Click OK.
- 2. For Firefox version 23 or higher, do the following.
 - a. In the address bar, type about: config and press ENTER.
 - b. Click I'll be careful, I promise!.

c. Verify that the **Value** of **Preference Name javascript.enabled** is set to **true**.

Deep Discovery Inspector hardware appliance installation

- Trend Micro provides a bare metal server with Deep Discovery Inspector pre-installed.
- Trend Micro provides Deep Discovery Inspector packaged as an ISO file on an installation DVD.

Install the Deep Discovery Inspector software on a bare metal server that meets the requirements listed in *Hardware appliance installation requirements on page 3-14*.

Installing Deep Discovery Inspector on hardware appliances with an optical drive

Procedure

1. Back up any pre-existing data on the target hard drive before installing Deep Discovery Inspector.

The installation process formats and repartitions the hard drive and removes all existing data.

) Тір

If you are reinstalling Deep Discovery Inspector, you can back up your current settings by going to Administration > System Maintenance > Backup / Restore in the Deep Discovery Inspector management console.

- 2. Connect a VGA screen to the video connector of the appliance.
- **3.** Insert the Deep Discovery Inspector installation DVD into the CD/DVD drive.

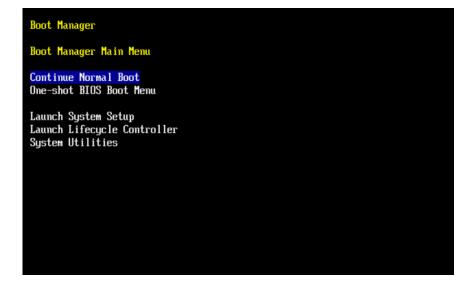
4. Turn on the appliance.

The **BIOS** screen appears.

```
F2 = System Setup
F10 = Lifecycle Controller (Config iDRAC, Update FW, Install OS)
F11 = Boot Manager
F12 = PXE Boot
Initializing Intel(R) Boot Agent XE v2.3.34.2
PXE 2.1 Build 092 (WfM 2.0)
Initializing Serial ATA devices...
-
```

5. Press F11.

The Boot Manager appears.



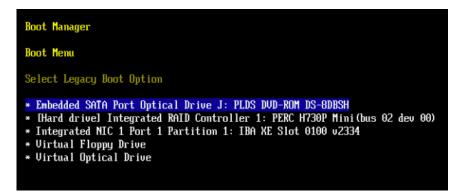
6. Select BIOS Boot Menu and press ENTER.



Important

When installing Deep Discovery Inspector through a serial connection, press ESC and simultaneously press **SHIFT** and 1 to enter the BIOS Boot Manager.

The **BIOS Boot Manager** appears.



7. Select TSSTcorp DVD-ROM SN-108BB and press ENTER.

The **Installation DVD** screen appears.

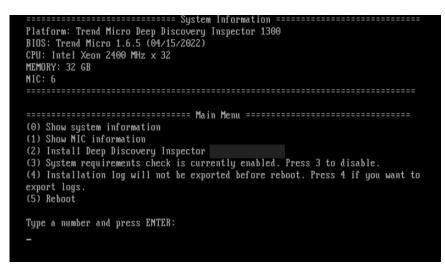
```
Trend Micro Deep Discovery Inspector
Installation DVD
Welcome to Deep Discovery Inspector
(1) Start the installation process
(2) Automatically evaluate and mirror network environment setup.
Type a number and press [ENTER].
The installation proceeds with the default option (1) if there is no option
chosen after 15 seconds.
```

8. Press ENTER.

Important

When installing Deep Discovery Inspector through a serial connection, type serial and press ENTER

The System Information screen appears.



9. For trial deployments, type **3** and press **ENTER** to skip the system requirements check.



By default, the installer checks system requirements before installing Deep Discovery Inspector to confirm that the appliance has the necessary resources to run the product.

- **10.** If you need to obtain installation logs for troubleshooting, type **4** and press ENTER.
- 11. Start the installation by typing 2 and pressing ENTER.

The Management Port Selection screen appears.

Deep Discovery Inspector automatically detects the active link cards (indicated by Link UP) available for use as a management port.

Hanagement Fort Selection Select an active link card to use for the management port. If unsure which one is connected to your management domain: 1. Disconnect all network cables. 3. Select Re-detect below. Select the card if it displays. 4. If the card cannot be selected, repeat steps 1 to 3.					
DuBoard Port 1 Link DUM. Intel Corporation 1350 Gigabit Network Connecti DuBoard Port 2 Link DUM. Intel Corporation 1350 Gigabit Network Connecti DuBoard Port 3 Link DUM. Intel Corporation 1350 Gigabit Network Connecti DuBoard Port 4 Link DUM. Intel Corporation 1350 Gigabit Network Connecti Diot 7 Port 1 Link DUM. Intel Corporation 1350 Gigabit Network Connecti Siot 7 Port 2 Link DUM. Intel Corporation 1350 Gigabit Network Connecti Diot 7 Port 2 Link DUM. Intel Corporation 1350 Gigabit Network Connecti Diot 7 Port 2 Link DUM. Intel Corporation 1350 Gigabit Network Connecti Diot 1 Port 2 Link DUM. Intel Corporation 1550 Gigabit Network Connecti Diot 1 Port 2 Link DUM. Intel Corporation Ethernet Controller X710 for Diot 1 Port 2 Link DUM. Intel Corporation Ethernet Controller X710 for - 1(*) 71z-					
	C OK > (Re-detect)				

FIGURE 4-1. Management Port Selection

Important

4-8

You cannot select ports from an inline NIC as the management port.

- Management Port Selection Select an active link card to use for the management port. If unsure which one is connected to your management domain: 1. Disconnect all network cables. 2. Connect one cable to one network port. 3. Select Re-detect below. Select the card if it displays. 4. If the card cannot be selected, repeat steps 1 to 3.				
Integrated Port 1 Integrated Port 2 Integrated Port 3	Link UP . Broadcom Inc. and subsidiaries NetXtreme BCH Link DOWN. Broadcom Inc. and subsidiaries NetXtreme BCM Link DOWN. Intel Corporation I350 Gigabit Network Conne			
	K OK > KRe-detect>			

12. Verify that the network port status and the actual port status match.

If a status conflict exists, select Re-detect and press ENTER.

13. Check which active link card connects to the management domain by doing the steps listed on the **Management Port Selection** screen.

14. Select an active link card and press ENTER.

The installation continues and completes.

- **15.** If you enabled installation log export on the **System Information** screen, save the installation logs.
 - a. Select a storage device and press ENTER.

If your storage device is not listed, Go to **Re-detect** and press **ENTER** to refresh the list.

b. When the installation log file name appears, press ENTER.

Record the file name for future reference. The file name uses the following format:

install.log.YYYY-MM-DD-hh-mm-ss



Tip

Trend Micro recommends saving exported installation logs to **sda11**.

The system automatically restarts and the Preconfiguration Console appears. If used, the installation DVD ejects from the CD/DVD drive.

- 16. (Optional) Remove the DVD to prevent reinstallation.
- 17. Configure the Deep Discovery Inspector network settings.
 - Access the preconfiguration console and change the device settings.

For details, see Preconfiguration on page 10-1.

• Open the management console and change the appliance IP settings.

For details, see the *Get Started* chapter of the *Deep Discovery Inspector Administrator's Guide*.

What to do next

See the *Deep Discovery Inspector Administrator's Guide* for details about configuring and administering Deep Discovery Inspector.

) Тір

Trend Micro recommends that you configure iDRAC (Integrated Dell Remote Access) on the appliance to allow remote system management and troubleshooting.

Installing Deep Discovery Inspector on hardware appliances without an optical drive

Procedure

1. Back up any pre-existing data on the target hard drive before installing Deep Discovery Inspector.

The installation process formats and repartitions the hard drive and removes all existing data.

) Tip

If you are reinstalling Deep Discovery Inspector, you can back up your current settings by going to **Administration** > **System Maintenance** > **Backup / Restore** in the Deep Discovery Inspector management console.

- 2. Download the Deep Discovery Inspector installation ISO from the Business Success Portal at <u>https://success.trendmicro.com/dcx/s/license</u>.
- **3.** Enable the iDRAC Direct USB port in the **Integrated Devices** screen of the BIOS of the Deep Discovery Inspector appliance.
- 4. Connect your computer to the Deep Discovery Inspector appliance using a USB to micro-USB cable and access the iDRAC interface over the USB port.

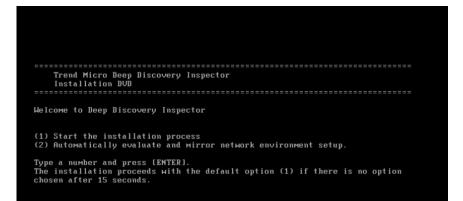
4-11

For more information, see the dell documentation at https:// www.dell.com/support/kbdoc/en-us/000130077/.

Use the virtual media function on iDRAC9 to launch the Deep Discovery 5. Inspector installer.

For more information, see the dell documentation at https:// www.dell.com/support/kbdoc/en-us/000124001/.

The Installation DVD screen appears.



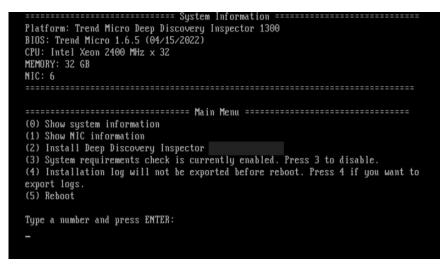
Press ENTER. 6.



Important

When installing Deep Discovery Inspector through a serial connection, type serial and press ENTER

The System Information screen appears.



7. For trial deployments, type **3** and press **ENTER** to skip the system requirements check.



By default, the installer checks system requirements before installing Deep Discovery Inspector to confirm that the appliance has the necessary resources to run the product.

- **8.** If you need to obtain installation logs for troubleshooting, type **4** and press ENTER.
- 9. Start the installation by typing 2 and pressing ENTER.

The Management Port Selection screen appears.

Deep Discovery Inspector automatically detects the active link cards (indicated by Link UP) available for use as a management port.

Hanagement Fort Selection Select an active link card to use for the management port. If unsure which one is connected to your management domain: 1. Bisconnect all network cables. 2. Connect one cable to one network port. 3. If the card cannot be selected, reveat steps 1 to 3.				
	C OK > CRe-detect>			

FIGURE 4-2. Management Port Selection



You cannot select ports from an inline NIC as the management port.

one is connected to 1. Disconnect all m 2. Connect one cable 3. Select Re-detect 4. If the card canne	to one network port. below. Select the card if it displays. of be selected, repeat steps 1 to 3.
Integrated Port 1 Integrated Port 2	Link UP . Broadcom Inc. and subsidiaries NetXtreme BCf Link DUWN. Intel Corporation I350 Gigabit Network Conne Link DUWN. Intel Corporation I350 Gigabit Network Conne
	K OK > KRe-detect>

10. Verify that the network port status and the actual port status match.

If a status conflict exists, select **Re-detect** and press ENTER.

11. Check which active link card connects to the management domain by doing the steps listed on the **Management Port Selection** screen.

12. Select an active link card and press ENTER.

The installation continues and completes.

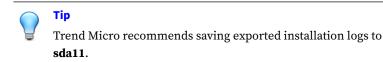
- **13.** If you enabled installation log export on the **System Information** screen, save the installation logs.
 - a. Select a storage device and press ENTER.

If your storage device is not listed, Go to **Re-detect** and press **ENTER** to refresh the list.

b. When the installation log file name appears, press ENTER.

Record the file name for future reference. The file name uses the following format:

install.log.YYYY-MM-DD-hh-mm-ss



The system automatically restarts and the Preconfiguration Console appears. If used, the installation DVD ejects from the CD/DVD drive.

- 14. (Optional) Remove the DVD to prevent reinstallation.
- 15. Configure the Deep Discovery Inspector network settings.
 - Access the preconfiguration console and change the device settings.

For details, see Preconfiguration on page 10-1.

• Open the management console and change the appliance IP settings.

For details, see the *Get Started* chapter of the *Deep Discovery Inspector Administrator's Guide*.

What to do next

Tip

See the *Deep Discovery Inspector Administrator's Guide* for details about configuring and administering Deep Discovery Inspector.

Trend Micro recommends that you configure iDRAC (Integrated Dell Remote Access) on the appliance to allow remote system management and troubleshooting.

Restoring to factory mode

Reset Deep Discovery Inspector by restoring the default settings that shipped with the product.

Procedure

1. Power on Deep Discovery Inspector with a monitor connected to a VGA port.

When Deep Discovery Inspector is starting and before the Preconfiguration Console opens, the **Press ESC key to enter the menu** prompt appears. If no action is performed, the system will automatically boot within 10 seconds.

- 2. Press the ESC key to enter the boot system options menu.
- 3. Using the arrow key, select **Restore to factory mode** and press ENTER.

Deep Discovery Inspector restarts and the Preconfiguration Console opens.

4-15



Chapter 5

Port mirroring on a VMware virtual distributed switch

Deep Discovery Inspector can monitor mirrored traffic using virtual distributed switches. Learn how to create a virtual distributed switch and configure Deep Discovery Inspector hardware appliances to monitor mirrored traffic in the following sections.

- Creating a VMware vSphere distributed switch (VDS) on page 5-2
- Deep discovery inspector hardware appliance with a VDS on page 5-5

Creating a VMware vSphere distributed switch (VDS)

Procedure

- 1. Create a new virtual distributed switch.
 - **a.** Log in to the vSphere Web Client.
 - b. Click Networking.
 - c. In the left panel, select your data center.
 - d. In the right panel, click the Create a new distributed switch icon.The New Distributed Switch window appears.
 - e. Type a name for the switch and then click Next.
 - f. Select the distributed switch version and then click **Next**.
 - **g.** For **Number of uplinks**, set at least **2** if your SPAN traffic is on a dedicated NIC. Otherwise, set this value to **1**.



Trend Micro recommends using a dedicated NIC.

- h. For Network I/O Control, select one of the following options.
 - **Disabled**: If your SPAN traffic on a dedicated NIC.



Trend Micro recommends using a dedicated NIC.

- **Enabled**: If your SPAN traffic is on the same NIC as your monitored traffic.
- i. Uncheck Create a default port group.
- j. Click Next.

5-2

- **k.** Verify that the summary information is correct and then click **Finish**.
- 2. Configure the virtual switch.
 - **a.** Right-click the virtual distributed switch you created in the previous steps, and then select **Settings** > **Edit Settings**.

The Edit Settings window appears.

b. Click Advanced.

The advanced settings appear.

- c. For MTU (Bytes), specify 1600.
- 3. Add port groups to the virtual distributed switch.
 - a. Click Networking.
 - Right-click the virtual distributed switch you created in the previous steps, and then select Distributed Port Group > New Distributed Port Group.

The New Distributed Port Group window appears.

- **c.** Type a name for the port group and then click **Next**.
- d. For Port binding, select Static binding.
- e. For Port allocation, select Fixed.
- **f.** For **Number of ports**, type the number of ports that you want to connect.
- g. Click Next.
- **h.** Verify that the settings on the summary screen are correct and then click **Finish**.

The new port group appears on the Manage tab.

- 4. (Optional) Repeat step 3 to add additional port groups.
- 5. Add an ESXi host to the virtual distributed switch.

a. Right-click the virtual switch you created in the previous steps, and then select **Add and Manage Hosts**.

The Add and Manage Hosts window appears.

- **b.** For Select task, select Add host and manage host networking (advanced).
- c. Click Next.
- d. For Select hosts, click + New hosts to add managed ESXi hosts.
- e. Click Next.
- f. For Selet network adapter tasks, add a checkmark to Manage physical adapters and Migrate virtual machine networking.
- g. Click Next.
- **h.** For **Manage physical network adapters**, manage the physical network adapters according to your network environment.
- i. Click Next.
- j. For Analyze impact, specify No impact.
- k. Click Next.
- **1.** For **Migrate VM networking**, migrate the VM networking according to your network environment.
- m. Click Next.
- n. For Ready to complete, click Finish.

The Add and Manage Hosts window closes.

o. Click the virtual switch you created in the previous steps, click the **Configure** tab, and then click **Topology** to verify the virtual switch topology that you configured.

Deep discovery inspector hardware appliance with a VDS

Deep Discovery Inspector hardware appliances can monitor mirrored traffic from a virtual distributed switch using encapsulated remote mirroring or remote mirroring. Learn how to configure Deep Discovery Inspector and the virtual distributed switch in the following sections.

- Hardware appliance configuring mirrored traffic monitoring from a VDS with encapsulated remote mirroring on page 5-5
- Hardware appliance configuring mirrored traffic monitoring from a VDS with remote mirroring on page 5-9

Hardware appliance - configuring mirrored traffic monitoring from a VDS with encapsulated remote mirroring

Encapsulated Remote Mirroring enables you to monitor traffic on multiple network interfaces or VLANs and send the monitored traffic to one or more destinations.

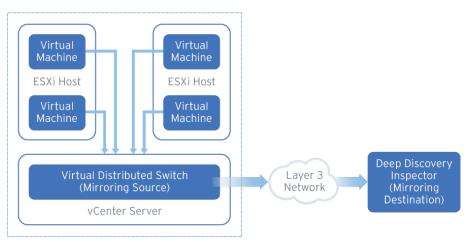


FIGURE 5-1. Mirrored Traffic Monitoring from a VDS with Encapsulated Remote Mirroring

By default, encapsulated remote mirroring on the virtual switch uses the management VMkernel port of the ESXi host as the encapsulation source IP address.

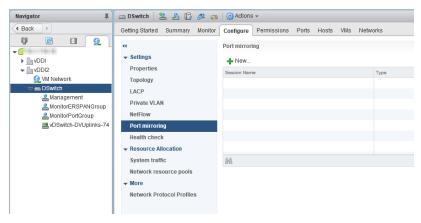
In the steps below, the mirroring source and mirroring destination are the following:

- Mirroring source: Virtual distributed switch that forwards mirrored traffic
- Mirroring destination: Deep Discovery Inspector

Procedure

- **1.** Configure the mirroring source to forward encapsulated remote mirrored traffic.
 - a. Log in to the vSphere Web Client.
 - **b.** Select your virtual distributed switch in the left column and then click **Configure**.
 - c. Click Port Mirroring.

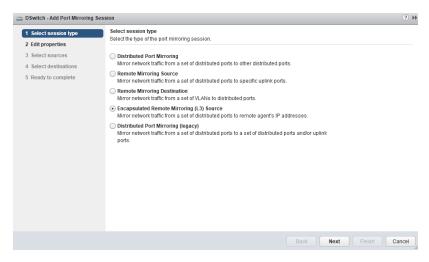
The **Port mirroring** screen appears.



d. Click New....

5-6

The Add Port Mirroring Sessions window appears.



- e. Select Encapsulated Remote Mirroring (L3) Source.
- f. Click Next.

The Edit properties screen appears.

DSwitch - Add Port Mirroring	Session		(?) H
1 Select session type 2 Edit properties	Edit properties Specify a name and the proper	rties of the port mirroring session.	
3 Select sources 4 Select destinations 5 Ready to complete	Name: Status: Session type: Encapsulation type: Session ID: Advanced properties Mirrored packet length (Bytes Sampling rate: Description:	erspan Enabled • Encapsulated Remote Mirroring (L3) Source GRE • 0 * 0 * 1 * 1	
		Back Next Finish Ca	ncel

g. In Name, type a session name.

- h. For Status, select Enabled.
- i. For Encapsulation type, select the encapsulation type.

🛉 Note

Using **ERSPAN THREE** may cause issues. Trend Micro recommends using **GRE** or **ERSPAN TWO**

j. Click Next.

The Select sources screen appears.

k. Click the plus icon

(

1

) to add the source virtual machines that you want to monitor.

I. Click Next.

The **Select destinations** screen appears.

m. Click the plus icon to add an IP address as a destination.

note

The destination IP address is the address that you configure on Deep Discovery Inspector in the next step.

n. Click Next.

The **Ready to complete** screen appears.

- o. Verify that the settings are correct and then click Finish.
- **2.** Configure the mirroring destination to receive encapsulated remote mirrored traffic.
 - a. In the Deep Discovery Inspector console, go to Administration > System Settings > Network Interface.

The **Network Interface** screen appears.

b. Locate a data port, and then click the right arrow (

) at the beginning of the row.

- c. Select Encapsulated Remote Mirroring.
- d. Specify the encapsulated remote mirroring destination address.



The encapsulated remote mirroring destination address must be routable from the management VMkernel port of the ESXi host.

e. Click Save.

Hardware appliance - configuring mirrored traffic monitoring from a VDS with remote mirroring

Remote mirroring enables you to monitor traffic on one switch through a device on another switch and send the monitored traffic to one or more destinations.

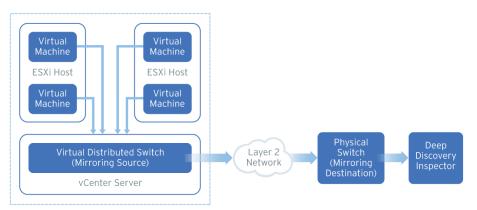


FIGURE 5-2. Mirrored Traffic Monitoring from a VDS with Remote Mirroring

Remote mirroring requires that you configure a remote mirroring VLAN on your physical switches. If you cannot configure a remote mirroring VLAN, consider using encapsulated remote mirroring as an alternative.

In the steps below, the mirroring source and mirroring destination are the following:

- Mirroring source: Virtual distributed switch that fowards mirrored traffic
- Mirroring destination: Physical switch that receives mirrored traffic and that can route the traffic to Deep Discovery Inspector

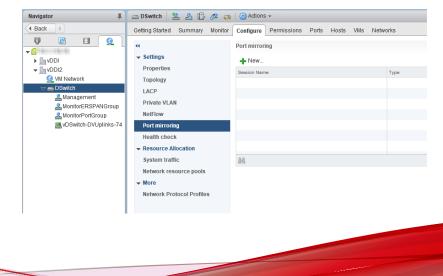
Before you begin, verify that the uplink ports of the ESXi hosts that receive traffic are linked to the physical switch trunk port.

Procedure

5-10

- **1.** Configure the mirroring source to forward remote mirrored traffic to the destination.
 - **a.** Log in to the vSphere Web Client.
 - **b.** Select your virtual distributed switch in the left column and then click **Configure**.
 - c. Click Port Mirroring.

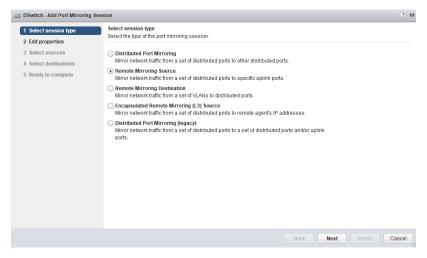
The **Port mirroring** screen appears.



5-11

d. Click New....

The Add Port Mirroring Sessions window appears.



- e. Select Remote Mirroring Source.
- f. Click Next.

The Edit properties screen appears.

DSwitch - Add Port Mirroring Ses	sion		? »
DSwitch - Add Port Mirroring Ses 1 Select session type 2 Edit properties 3 Select sources 4 Select destinations 5 Ready to complete	sion Edit properties Specify a name and the properties of Name: Status: Session type: Encapsulation VLAN ID: Advanced properties Normal VO on destination ports: Mirrored packet length (Bytes): Sampling rate: Description:	If the port mirroring session.	•
		Back Next F	Finish Cancel

- g. In Name, type a session name.
- h. For Status, select Enabled.
- i. In Encapsulation VLAN ID, specify the VLAN ID.



j. Click Next.

The Select sources screen appears.

k. Click the plus icon

†]

) to add the source virtual machines that you want to monitor.

I. Click Next.

The Select destinations screen appears.

m. Add uplink in Available uplinks to Selected uplinks.

5-13

n. Click Next.

The Ready to complete screen appears.

- o. Verify that the settings are correct and then click **Finish**.
- **2.** Configure the mirroring destination to forward encapsulated remote mirrored traffic to Deep Discovery Inspector.

Part III

Virtual appliance installation and deployment





6-1

Chapter 6

Virtual appliance deployment

Learn tips, suggestions, and requirements for installing a Deep Discovery Inspector virtual appliance in the following sections.

Deployment overview

Procedure

- Plan the deployment. See Virtual appliance deployment planning on page 6-2.
- **2.** Review the installation requirements.

See Virtual appliance installation requirements on page 6-4.

- Review the system requirements.
 See Virtual appliance system requirements on page 6-5.
- 4. Create a virtual appliance.See *Create a new virtual appliance on page 7-1*.
- 5. Install Deep Discovery Inspector.

See Deep Discovery Inspector virtual appliance installation on page 8-4.

6. Preconfigure Deep Discovery Inspector.

See Preconfiguration on page 10-1.

Virtual appliance deployment planning

Plan how to best deploy Deep Discovery Inspector by doing the following:

- Determine the segments of your network that need protection.
- Plan for network traffic, considering the location of appliances critical to your operations such as email, web, and application servers.
- Determine both the number of appliances needed to meet your security needs and their locations on the network
- Conduct a pilot deployment on a test segment of your network.
- Redefine your deployment strategy based on the results of the pilot deployment.

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

Deployment scenarios

Deep Discovery Inspector can be deployed as a hardware appliance or as a virtual appliance.

- Hardware appliance: Deep Discovery Inspector can be deployed either inline or out-of-band.
 - Inline: Deep Discovery Inspector acts as a transparent bridge and can inspect decrypted TLS traffic. When deployed inline, only traffic flowing through the inline ports is inspected.



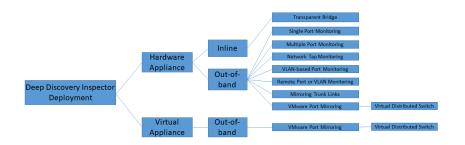
Note

Installing an additional inline (LAN bypass) network interface card is needed for inline deployment. For installation instructions and compatible Deep Discovery Inspector appliance models, refer to the *Inline (LAN Bypass) Network Interface Card Installation Guide*.

- Out-of-band: Deep Discovery Inspector monitors network traffic by connecting to the mirror port on a switch for minimal to no network interruption. When deployed out-of-band, only traffic mirrored to the data ports is inspected.
- Virtual appliance: Deep Discovery Inspector can only be deployed out-of-band. Deep Discovery Inspector monitors network traffic by connecting to the mirror port on a switch for minimal to no network interruption.

6-3

The figure below provides a high-level overview of supported deployments.



VMware port mirroring

Use VMware port mirroring when traffic passes through a virtual distributed switch.

For more details, see *Port mirroring on a VMware virtual distributed switch on page 9-1*.

Virtual appliance installation requirements

Ensure the following before installing Deep Discovery Inspector.

REQUIREMENT	DESCRIPTION			
Match port speeds	The destination port speed should be the same as the source port speed to ensure equal port mirroring. If the destination port is unable to handle the faster speed of the source port, the destination port may drop some data.			

6-4

REQUIREMENT	DESCRIPTION			
Monitor all data	Deep Discovery Inspector monitors all inbound and outbound network traffic. Note To ensure Deep Discovery Inspector captures traffic from both directions, configure the mirror port, and make sure that traffic in both directions is mirrored to the port.			

Virtual appliance system requirements

Deep Discovery Inspector requires the following:

- Virtual host appliance requirements on page 6-5
- Management console requirements on page 3-16

Virtual host appliance requirements

You can install Deep Discovery Inspector on:

- VMware ESXi 7.0 or 8.0.
- Microsoft Hyper-V on Windows Server 2019 or 2022.
- KVM.

Deep Discovery Inspector virtual appliances do not support nested virtual machines. When using a Deep Discovery Inspector virtual appliance with Virtual Analyzer, only external Virtual Analyzers and Sandbox as a Service are supported.

Trend Micro recommends the following minimum specifications based on the throughput of your licensed model.

Throughput (Mbps)	VIRTUAL CPUs*	Virtual Memory (GB)	Virtual Disk (GB)	Virtual NICs**	SANDBOX AS A SERVICE SUPPORT
250	6	32	500	2	Yes
500	6	32	500	2	Yes
1000	12	32	1000	3	Yes

TABLE 6-1. Virtual Appliance Specifications



Note

- * Virtual CPUs require a minimum speed of 2.5 GHz with hyper-threading support, Virtualization Technology (VT), and 64-bit architecture.
- ** Trend Micro recommends using the VMXNET 3 network adapter on ESXi, and the VirtIO or E1000 network adapters on KVM.

Management console requirements

Deep Discovery Inspector provides a built-in online management console for viewing system status, configuring and viewing threat detections and logs, running reports, administering Deep Discovery Inspector, updating components, and obtaining help.

For details, see *Management Console* in the *Deep Discovery Inspector Administrator's Guide*.

The Deep Discovery Inspector management console supports the following web browsers:

- Google[™] Chrome[™]
- Mozilla[™] FireFox[™]
- Microsoft[™] Edge

Recommended resolution rate: 1280x800





Chapter 7

Create a new virtual appliance

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

- Create a VMware ESXi virtual appliance on page 7-2
- Create a Microsoft Hyper-V virtual appliance on page 7-14

For details about the minimum virtual host appliance system requirements and supported hypervisors, see *Virtual host appliance requirements on page* 6-5.

Create a VMware ESXi virtual appliance

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

- Requirements for a virtual machine in VMware ESXi on page 7-2
- Configuring the VMware ESXi server network on page 7-2
- Creating a virtual machine in VMware ESXi on page 7-7
- Enabling hardware-assisted virtualization in VMware ESXi on page 7-13

Requirements for a virtual machine in VMware ESXi



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.

To install Deep Discovery Inspector in a VMware ESXi server, ensure that your server has:

- VMware ESXi server version 7.0 or 8.0.
- Two or more NICs on the VMware ESXi server: one manager network, and at least one data network.

For details, see Configuring the VMware ESXi server network on page 7-2.

• Virtualization Technology (VT) enabled on your VMware host and in the VMware vSphere configuration.

For details about the VMware vSphere configuration, see *Enabling* hardware-assisted virtualization in VMware ESXi on page 7-13.

Configuring the VMware ESXi server network

Use a browser to connect the ESXi server.

Procedure

1. Sign into the VMware ESXi server.

vm w	are	
User name		
Password		vm ware' esxi

2. Go to Networking > Virtual switches. Observe the initial state.

📲 Navigator 🗉	. Networkin	g		
✓ Host	Port groups Virtual swite	ches Physical NICs VM	Ikernel NICs TCP/IP stacks	Firewall rules
Manage Monitor	🏝 Add standard virtual switch	🔜 Add uplink 🥒 Edit setting	is 🙋 Refresh 🔅 Action:	Q Search
🕶 🛱 Virtual Machines 🛛 🔽 7	Name ~	Port groups ~	Uplinks ~	Type ~
👻 😭 Hanana, Hilitia	switch0	2	1	Standard vSwitch
Monitor				
🕨 🞒 New Virtual Machine				1 items
More VMs				
Storage				
🛛 🔮 Networking 📃 🚺				

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

- a. For vSwitch Name, type Data Network.
- **b.** For **MTU**, type 1600.
- c. For Uplink 1, select a NIC card for a Data Network.
- d. Expand Security and configure the settings.
 - 1. For **Promiscuous mode**, select **Reject**.
 - 2. For MAC address changes, select Accept.
 - 3. For Forged transmits, select Accept.

Add standard virtual switch - Da	Network
Add uplink	
vSwitch Name	Data Network
MTU	1600
Uplink 1	vmnic5 - Down 🔻
Link discovery	Click to expand
▼ Security	
Promiscuous mode	O Accept Reject
MAC address changes	Accept Reject
Forged transmits	Accept Reject
	Add Cancel

e. Click Add.

7-4

Port groups Virtual switches	Physical NICs VMkernel NICs	TCP/IP stacks Firewall rules	
鼬 Add standard virtual switch 🛛 🔜	Add uplink 🥒 Edit settings \mid 🧲 Re	fresh 🛛 🔅 Actions	Q. Search
Name	 Port groups 	v Uplinks v	Туре
www.switch0	2	1	Standard vSwitch
Data Network	0	1	Standard vSwitch
			2 items

- 4. Click on the **Port groups** tab and observe the initial state.
- 5. Click Add port group and configure the settings.

📲 Navigator 🗆	- Networkin	ng							
▼ 🗒 Host	Port groups Virtual swite	ches Phy	sical NICs	VMkernel NICs	TCP/II	P stacks	Firewall rules		
Manage Monitor	👲 Add port group 🥒 Edit	settings 🛛 C	Refresh	Actions			Q Search		
▼	Name ~	Active ~	VLAN ID \sim	Туре	~	vSwitch	~	VMs	~
👻 🚰 Timothy_DDI5.0	VM Network	2	0	Standard port group		switch0 www.ch0		7	
Monitor	Management Network	1	0	Standard port group		switch0 witch0		N/A	
 New Virtual Machine More VMs 								2 iten	15
→ 🗐 Storage									A
🔮 Networking 📃 🚺	4								

- a. For Name, type Data Port Group.
- **b.** For **VLAN ID**, type 4095.
- c. For Virtual switch, select a Data Network.

일 Add port group - Data Port	Group	
Name	Data Port Group	
VLAN ID	4095	
Virtual switch	Data Network	
► Security	Click to expand	
		Add Cancel

- **d.** Expand **Security** and configure the settings.
 - 1. For **Promiscuous mode**, select **Accept**.
 - 2. For both Mac Address changes and Forged transmits, select Inherit from vSwitch.

🔮 Add port group - Data Port Group	
Name	Data Port Group
VLAN ID	4095
Virtual switch	Data Network
✓ Security	
Promiscuous mode	● Accept ● Reject ● Inherit from vSwitch
MAC address changes	O Accept O Reject Inherit from vSwitch
Forged transmits	CAccept Reject Inherit from vSwitch
	Add Cancel

6. Click Add.

7-6

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

Eait setting	Data port group	-			
3	Accessible: Virtual machines: Virtual switch:	Yes			
	VLAN ID: Active ports:	4095 0			
vSwitch top	ology		 		
🧕 Data port	group			Physical adapter	S
VLAN ID:	4095			vmnic5	

Creating a virtual machine in VMware ESXi

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.

🔁 New virtual machine			
1 Select creation type 2 Select a name and guest OS 3 Select storage 4 Customize settings	Select creation type How would you like to create a Virtual Machine?		This option guides you through creating a new virtual
5 Ready to complete	Celetar They without nachine Deploy a virtual machine from an OVF or OVA file Register an existing virtual machine	~	machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.
vm ware [.]			Back Next Finish Cancel

- 3. On the Select a name and guest OS screen, configure the settings.
 - a. For Name, type New Virtual Machine.
 - b. For Compatibility, select ESXi 7.0.
 - c. For Guest OS family, select Linux.

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

Select creation type	Select a name and gu	lest OS	
Select a name and guest OS Select storage	Specify a unique name and OS		
Customize settings Ready to complete	Name		
Ready to complete	New Virtual machine		
	Virtual machine names can conta	in up to 80 characters and they must be unique within each	ESXi instance.
	Identifying the guest operating sy- installation.	stem here allows the wizard to provide the appropriate defau	Its for the operating syst
	Compatibility	ESXi 7.0 U1 virtual machine	~
	Guest OS family	Linux	~
	Guest OS version	Harden T der der	~
	1		
vm ware [*]			

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

1 Select creation type	Select storage										
2 Select a name and guest OS 3 Select storage	Select the storage type an	d datastore									
4 Customize settings 5 Ready to complete	Standard Persisten Select a datastore for th		configuration	files	and all of	its' vi	rtual disks.				
	Name	~		~	Free	~	Туре	~	Thin pro ~	Access	`
	datastore1		6.42 TB		5.9 TB		VMFS6		Supported	Single 1 iten	ne
vm ware [.]											

- 6. Configure the settings on the **Customize settings** screen.
 - **a.** For **CPU**, select the CPU amount based on the throughput of your Virtual Deep Discovery Inspector license.
 - For 250 or 500 Mbps throughput, select at least **6** CPUs
 - For 1000 Mbps throughput, select at least **12** CPUs
 - **b.** For **Memory**, select at least **32 GB** of memory for the virtual machine.
 - **c.** For **Hard disk**, select the hard disk size based on the throughput of your Virtual Deep Discovery Inspector license.
 - For 250 or 500 Mbps throughput, select at least 500 GB
 - For 1000 Mbps throughput, select at least 1000 GB
 - d. For SCSI Controller 0, select LSI Logic Parallel.
 - e. For **Network**, configure the amount of NICs based on the throughput of your Virtual Deep Discovery Inspector license.
 - For 250 or 500 Mbps throughput, configure at least 2 NICs
 - For 1000 Mbps throughput, configure at least 3 NICs
 - 1. Set the VMware ESXi server **VM Network** as the Deep Discovery Inspector Management Network (NIC 1).
 - 2. Set the **Data port group** as the Deep Discovery Inspector Data Network (NIC 2).

1 Select creation type 2 Select a name and guest OS 3 Select storage	Customize settings Configure the virtual machine hardwa	ire and virtual machine additional options						
4 Customize settings 5 Ready to complete	🔜 Add hard disk 🛛 🗯 Add network adapter 🗧 Add other device							
	▶ 🖬 CPU 🛕	6 ~ ()						
	🕨 🛲 Memory 🧥	32 GB ~						
	🕨 🖾 Hard disk 1 🧥	500 GB ~	Э					
	F SS SCSI Controller 0	LSI Logic Parallel ~	Э					
	SATA Controller 0	6	Э					
	USB controller 1	USB 2.0 ~	Э					
	* INI Network Adapter 1	VM Network ~	Э					
	Status	Connect at power on						
	Adapter Type	VMXNET 3 ~						
	MAC Address	Automatic v 00:00:00:00:00						
	- Mill New Network Adapter	Data port group 🗸	Э					
vm ware	Status	Connect at nower on						

Note

Trend Micro recommends using the VMXNET 3 network adapter on ESXi 7.0 or 8.0.

- 7. Click Next.
- 8. On the Ready to complete screen, review the settings and click Finish.

lect creation type lect a name and guest OS	Ready to complete	
ect storage	Review your settings selection befo	e hnishing the witzard
stomize settings ady to complete	Name	New Virtual machine
ay to complete	Datastore	9_DS_16T
	Guest OS name	CentOS 7 (64-bit)
	Compatibility	ESXi 6.5 virtual machine
	vCPUs	6
	Memory	32 GB
	Network adapters	2
	Network adapter 1 network	VM Network
	Network adapter 1 type	VMXNET 3
	Network adapter 2 network	Data port group
	Network adapter 2 type	VMXNET 3
	IDE controller 0	IDE 0
	IDE controller 1	DE 1
	SCSI controller 0	LSI Logic Parallel
	SATA controller 0	New SATA controller
vm ware	Hard disk 1	
	Capacity	500GB
	Datastore	[9_DS_16T] New Virtual machine/
	Mode	Dependent

9. Enable hardware-assisted virtualization in the VMware Sphere Web Client.

For details, see *Enabling hardware-assisted virtualization in VMware ESXi* on page 7-13.

- **10.** In the VMWare vSphere web client, right-click the virtual machine and select **Edit Settings**.
- **11.** Go to **VM Options** > **Boot Options**.
- 12. Ensure Firmware is set to BIOS.

7-12

Virtual Hardware VM Options	
> General Options	VM Name: Tom_ddi 6.5 EN (10.209.26.143)
VMware Remote Console Options	
>	Lock the guest operating system when the last remote user disconnect
> Encryption	Expand for encryption settings
> Power management	Expand for power management settings
> VMware Tools	Expand for VMware Tools settings
✓ Boot Options	
Firmware	BIOS (recommended) V
Boot Delay	When powering on or resetting, delay boot order by
	0 milliseconds
Force BIOS setup	$\hfill\square$ During the next boot, force entry into the BIOS setup screen
Failed Boot Recovery	□ If the VM fails to find boot device, automatically retry after
	10 seconds

Enabling hardware-assisted virtualization in VMware ESXi

Procedure

1. Verify that Virtualization Technology (VT) is enabled on the VMware host.

Тір

The Virtualization Technology setting is typically in the BIOS settings and the location varies based on the system vendor. The feature may be named AMD-V, VT, VT-x, Vanderpool Technology, Virtualization Technology, VMX, or Virtual Machine Extensions.

- 2. In the VMware vSphere Web Client, right-click the virtual machine and select **Edit Settings**.
- 3. On to the Virtual Hardware tab, expand CPU.

- 4. Enable **Expose hardware-assisted virtualization to guest OS**.
- 5. Click OK.

Create a Microsoft Hyper-V virtual appliance

Learn how to create a virtual appliance using Microsoft Hyper-V in the following topics:

- Creating a virtual machine in Microsoft Hyper-V on page 7-14
- Configure traffic mirroring in Microsoft Hyper-V on page 7-36

Creating a virtual machine in Microsoft Hyper-V



Important

Deep Discovery Inspector virtual appliances installed on a Microsoft Hyper-V virtual machines do not support UEFI generation 2.



Important

Deep Discovery Inspector only supports installation on Hyper-V virtual machines running on Windows Server 2019 or 2022.

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.



ile	Action View Help		
•	New	>	
H	Import Virtual Machine	25	Actions
	Hyper-V Settings	State CPU Usage Assigned Memory Uptime Status	WIN-2PFLUH4Q1Q
	Virtual Switch Manager		New
	Virtual SAN Manager	No virtual machines were found on this server.	🐴 Import Virtual Machine
	Edit Disk		Hyper-V Settings
	Inspect Disk		🟭 Virtual Switch Manager
	Stop Service		🔬 Virtual SAN Manager
	Remove Server		🚄 Edit Disk
	Refresh		🔄 Inspect Disk
	Help		Stop Service
		No viitual machine selected.	× Remove Server
			🖏 Refresh
			View
			Help
	Details		
		No item selected	
		No Kell solicited.	

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**.

🚰 Virtual Switch Manager foi	X
Virtual Switches New virtual network switch Global Network Settings MAC Address Range	Create virtual switch What type of virtual switch do you want to create? External Internal Private
	Create Virtual Switch Creates a virtual switch that binds to the physical network adapter so that virtual machines can access a physical network.
	OK Cancel Apply

d. Click Create Virtual Switch.

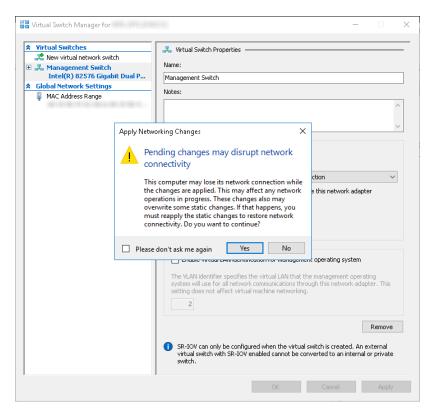
The Virtual Switch Properties screen appears.

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

Virtual Switches	👗 Virtual Switch Properties —					
💐 New virtual network switch						
🚜 Management Switch	Name:					
Intel(R) 82576 Gigabit Dual P Global Network Settings	Management Switch					
MAC Address Range	Notes:					
	· · · · · · · · · · · · · · · · · · ·					
	Connection type					
	What do you want to connect this virtual switch to?					
	External network:					
	Intel(R) 82576 Gigabit Dual Port Network Connection					
	Allow management operating system to share this network adapter					
	Enable single-root I/O virtualization (SR-IOV)					
	O Internal network					
	Private network					
	VLAN ID					
	Enable virtual LAN identification for management operating system					
	The VLAN identifier specifies the virtual LAN that the management operating					
	system will use for all network communications through this network adapter. This					
	setting does not affect virtual machine networking.					
	2					
	Remove					
	 SR-IOV can only be configured when the virtual switch is created. An external virtual switch with SR-IOV enabled cannot be converted to an internal or private switch. 					
	SYNCE I.					

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 Viritual Switch Properties screen appears.

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

n. Click Apply.

The Apply Networking Changes confirmation window appears.

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

The confirmation window closes.

- p. Click OK.
- 2. Create a virtual machine.
 - a. In Hyper-V Manager, go to Action > New > Virtual Machine.

(= =	New >	Virtual Machine		
	Import Virtual Machine Hyper-V Settings	Hard Disk Floppy Disk		Actions WIN-2PFLUH4Q1Q
	Virtual Switch Manager Virtual SAN Manager Edit Disk Inspect Disk Stop Service Remove Server	State CPU Usage Assigned Memory Uptime Status No virtual machines were found on this server.		New Import Virtual Machine Hyper-V Settings Virtual Savich Manager Virtual SAN Manager
	Refresh			Euli Disk Inspect Disk Stop Service
		No virtu	I machine selected.	X Remove Server Refresh View Help
	Details			
		Na	item selected.	

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 Inspector.

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

d. Click Next.

The **Specify Generation** screen appears.

e. Select Generation 1.

📃 New Virtual Machine Wiza	rd X
Specify Gene	ration
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	 Choose the generation of this virtual machine. ④ Generation 1 This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V. O Generation 2 This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system. More a virtual machine has been created, you cannot change its generation.
	< Previous Next > Finish Cancel

f. Click Next.

The Assign Memory screen appears.

g. For Startup memory, assign at least 32768 MB (32 GB).

🖳 New Virtual Machine Wizar	d	×
📒 Assign Memo	угу	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system. Startup memory: 32768 MB Use Dynamic Memory for this virtual machine. Use Dynamic Memory for this virtual machine. When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.	
	< Previous Next > Finish Cancel	

h. Click Next.

7-22

The **Configure Networking** screen appears.

i. For Connection, select Mangement Switch.

🖳 New Virtual Machine Wiza	rd	×
💹 Configure N	etworking	
Before You Begin Specify Name and Location Specify Generation Assign Memory	Each new virtual machine includes a network adapter. You can configure the network adapter to virtual switch, or it can remain disconnected. Connection: Management Switch	use a
Configure Networking Connect Virtual Hard Disk Installation Options Summary		
	< Previous Next > Finish Can	cel

j. Click Next.

The Connect Virtual Hard Disk screen appears.

k. Select Attach a virtual hard disk later.

🐖 New Virtual Machine Wiza	rd	×
Connect Vir	tual Hard Disk	
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Summary	A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties. C Create a virtual hard disk Use this option to create a VHDX dynamically expanding virtual hard disk. Name: Deep Discovery Inspector.vhdx Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse Size: 127 GB (Maximum: 64 TB) C Use an existing virtual hard disk Use this option to attach an existing virtual hard disk, either VHD or VHDX format. Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse Eccation: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse Eccation: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Eccation: Ec	
	 Attach a virtual hard disk later Use this option to skip this step now and attach an existing virtual hard disk later. 	
	< Previous Next > Finish Cancel	

I. Click Next.

The Completing the New Virtual Machine Wizard screen appears.

- **m.** Verify that the virtual machine configuration is correct and then click **Finish**.
- **3.** Create a virtual hard disk.
 - a. In Hyper-V Manager, select the Deep Discovery Inspector virtual machine and then go to **Action** > **New** > **Hard Disk**.



🔿 🖄 📾	iew Help								
Hyper-V Mana	iger	Virtual Machines					_ /	Actions	
WIN-POJO	New	Virtual Machines	Virtual Machine			11.0		WIN-P0JOKHBH75H	
	Import Virtual Machine		Hard Disk	Usage	Assigned Memory	Uptime	- F	New	_
	Hyper-V Settin	205	Floppy Disk				1	🔒 Import Virtual Machine	
	Virtual Switch	-						Hyper-V Settings	
	Virtual SAN M						8	Virtual Switch Manager	
Edit Disk Inspect Disk Stop Service Remove Server Refresh		-						🔬 Virtual SAN Manager	
								🚄 Edit Disk	
							>	Inspect Disk	
							Stop Service		
							× Remove Server		
	The selected virtual machine has no checkpoints.				🖏 Refresh				
	View > Help						View		
						- 11	? Help		
								Deep Discovery Inspector	
							16	📲 Connect	
								Settings	
		Deep Discovery					= 1	💿 Start	
		Deep Discovery	Inspector					heckpoint	
			Created: 8/28/2	018 10:15:2	5 PM Clustered:	No		Move	
			Configuration Version: 8.0					Export	
			Generation: 1 Notes: None					- Rename	
			Notes. Note					Delete	
								1 Enable Replication	
		Summary Memor	v Networking Replication				-11	Help	

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

b. Click **Next**.

The **Choose Disk Format** screen appears.

c. Select VHDX.

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

d. Click Next.

7-26

The **Choose Disk Type** screen appears.

e. Select Fixed size.

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

f. Click Next.

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

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

ắ New Virtual Hard Disk Wiza	d	×
🚢 Specify Name	and Location	
Before You Begin Choose Disk Format Choose Disk Type	Specify the name and location of the virtual hard disk file. Name: Deep Discovery Inspector vhdx	
Specify Name and Location	Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\	Browse
Configure Disk Summary		
	< Previous Next > Fi	inish Cancel

h. Click Next.

7-28

The **Configure Disk** screen appears.

- i. Select Create a New blank virtual hard disk.
- **j.** For **Size**, specify the following based on your Deep Discovery Inspector model.
 - For the 250 or 500 Mbps throughput models, specify at least 500 GB.
 - For the 1000 Mbps throughput model, specify at least 1000 GB.

Level Wirtual Hard Disk Wize	-	×
🚢 Configure Di	5K	
Before You Begin Choose Disk Format Choose Disk Type Specify Name and Location	You can create a blank virtual hard disk or copy the contents Create a new blank virtual hard disk Size: 1000[GB (Maximum: 64 TB) Copy the contents of the specified physical disk:	of an existing physical disk.
Configure Disk Summary	Physical Hard Disk \\.\PHYSICALDRIVE0 Copy the contents of the specified virtual hard disk Path:	Size 127 GB Browse
	< Previous Ne	xt > Finish Cancel

k. Click Next.

The Completing the New Virtual Hard Disk Wizard screen appears.

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



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 Inspector virtual machine and then go to **Action** > **Settings**.

∎a ⊢	Hyper-V N	/lanager											-	×	(
File	Action	View	Help												
-	C	onnect													
H	Se	ttings			chines							Actions			_
	St	art			Cimes		State	CPU Usage	Assigned	Managari I	Jptir	WIN-2PFLUH4Q1Q		•	^
	CI	neckpoir	ot		scover	Inspector		CPO Osage	Assigned	Memory L	pur	New		•	
			ic .			mopoordi	0.					强 Import Virtual Machine			
		ove port										📔 Hyper-V Settings			
		name										🟭 Virtual Switch Manager			
		elete										🔒 Virtual SAN Manager			
	5.	able Re	nlicatio									🥁 Edit Disk			
			pricado		ts							🔄 Inspect Disk			
	н	elp										 Stop Service 			
							The selected v	irtual machine ha	s no checkpo	iints.		🗙 Remove Server			
												🖏 Refresh			
												View		•	
												👔 Help			
												Deep Discovery Inspector		•	
											_	📲 Connect			
				Deep	Discovery	Inspector						🛅 Settings			
						Created		8/29/2018 7:46	-59 PM	Clustered: N	lo.	🙂 Start			
							ation Version:			clusteredi		🔂 Checkpoint			
						Generat	ion:	1				Move			
						Notes:		None				📮 Export			
												🛋 Rename			
												🛃 Delete			
				Summ	ary Memor	y Networ	king Replication	n			_	🚏 Enable Replication			
				<							>	👔 Help			~
Displa	ys the vir	tual mad	chine se	ettings us	er interface										

The settings window appears.

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

The **Processor** settings appear.

- **c.** For Number of virtual processors, specify the following based on your Deep Discovery Inspector model.
 - For the 250 or 500 Mbps throughput models, specify at least 6 virtual processors.
 - For the 1000 Mbps throughput model, specify at least 12 virtual processors.

Dee	ep Discovery Inspector 🛛 🗸 🗸	♦ ►
*	Hardware 🔨	Processor -
	📑 Add Hardware	
	BIOS Boot from CD	You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.
	Security Key Storage Drive disabled	Number of virtual processors: 12
	Memory	Resource control
	8192 MB	You can use resource controls to balance resources among virtual machines.
÷	Processor 12 Virtual processors	Virtual machine reserve (percentage): 0
=		Percent of total system resources: 0
_	IDE Controller 0 Hard Drive	Percent of total system resources:
	Deep Discovery Inspector	Virtual machine limit (percentage): 100
Ξ	IDE Controller 1	
	DVD Drive	Percent of total system resources: 150
	None	Relative weight: 100
	🗐 SCSI Controller	Relative Weight.
÷	📮 Network Adapter	
	Management Switch	1 This virtual machine is configured with the following:
	COM 1 None	Sockets: 3
	COM 2	NUMA nodes per socket: 1 Virtual processors per NUMA node: 4
	None	Memory per NUMA node: 3804 MB
	🔜 Diskette Drive	
	None	
۸.	Management	
	I Name	
	Deep Discovery Inspector	
	Some services	
	Checkpoints Production	
	Smart Paging File Location	
	C:\ProgramData\Microsoft\Win 🗸	

- 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**.

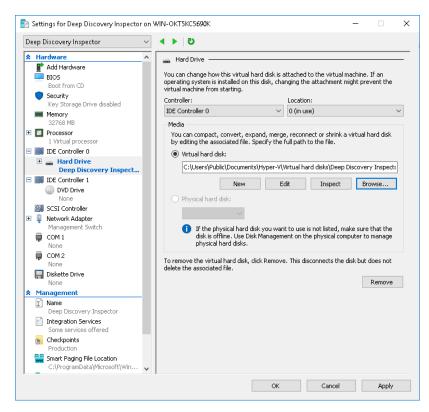
)e	eep Discovery Inspector	\sim	•		Ü									
*	Hardware	^		ID	E Contr	roller —								
	📑 Add Hardware		—·											
	EIOS					hard drive								
	Boot from CD		Se	elect	the typ	e of drive	e you wa	nt to a	tach to:	the co	ontrolle	er and th	en click A	Add.
	Security		H	lard (Drive									
	Key Storage Drive disabled		D	VD D	Drive									
	Memory													
	32768 MB													
+	Processor 1 Virtual processor													
	I Virtual processor													ب ب
_	IDE Controller 1													Add
_				ura	n confi	gure a ha	rd drive	to use	a virtual	bard	tick or	a obycic	al bard d	lick after
	DVD Drive						the con		a vii caai	nara	10100	a priysie	a na a a	
				iu au	tath th									
	None		^y 0	u au	tach th	e unve to		cronor.						
	SCSI Controller		0	u au	tach th	e unve to		cronor.						
F	SCSI Controller			iu aci	cach th	e unve to		cronor.						
ŧ	SCSI Controller Vetwork Adapter Management Switch		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	ju aci	cach th	e unve to								
ŧ	SCSI Controller		, ,0	iu au	tath th	e unve to								
ŧ	SCSI Controller Network Adapter Management Switch COM 1 None		, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	iu au	cach ch	e unve to								
ŧ	SCSI Controller Network Adapter Management Switch COM 1 None		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	iu au	cach ch	e unve to								
ŧ	SCSI Controller Network Adapter Management Switch COM 1 None COM 2		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		tach th	e unve to								
ŧ	 SCSI Controller Wetwork Adapter Management Switch COM 1 None COM 2 None 		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		tach th	e unve to								
	 SCSI Controller Network Adapter Management Switch COM 1 None COM 2 None Diskette Drive 		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		tach th	e unive cu								
	SCSI Controller Kanagement Switch COM 1 None COM 1 None Diskette Drive None Management X Name Management X Name		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		tach th	e unive cu								
	SCSI Controller Network Adapter Management Switch COM 1 None CoM 2 None Diskette Drive None Management Management None Deep Discovery Inspector		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		tach th	e unive cu								
	SCSI Controller Controller Management Switch Con 1 None Con 1 None Solution None Management None Deep Discovery Inspector Integration Services		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		tach th	e dinve co								
*	 SCSI Controller Wanagement Switch COM 1 None Diskette Drive None Diskette Drive None Management Name Deep Discovery Inspector Integration Services Some services offered 		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		tach th									
	 SCSI Controller Network Adapter Management Switch COM 1 None COM 2 None Diskette Drive None Management Management Nane Deep Discovery Inspector Integration Services Some services offered Checkpoints 		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	u au	tach th									
	SCSI Controller Controller Management Switch Con 1 None Con 2 None None Some Switch Drive None Management Name Deep Discovery Inspector Deep Discovery Inspector Integration Services Some services offered Checkpoints Production		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		tach th									
	 SCSI Controller Wanagement Switch COM 1 None Diskette Drive None Diskette Drive None Management Name Desp Discovery Inspector Integration Services Some services offrered Coeckpoints Production Smart Paging File Location 		y0		tach th									
	SCSI Controller Controller Management Switch Con 1 None Con 2 None None Some Switch Drive None Management Name Deep Discovery Inspector Deep Discovery Inspector Integration Services Some services offered Checkpoints Production		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		(ach dh									

g. Click Add.

The Hard Drive settings appear.

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

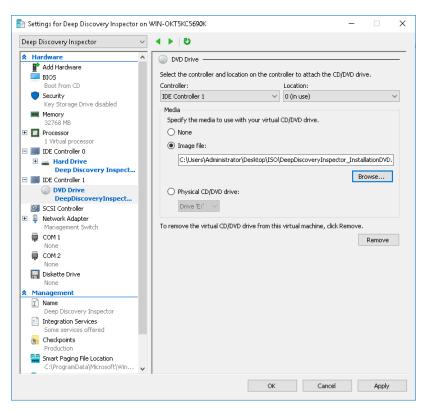
7-32



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

The DVD Drive settings appear.

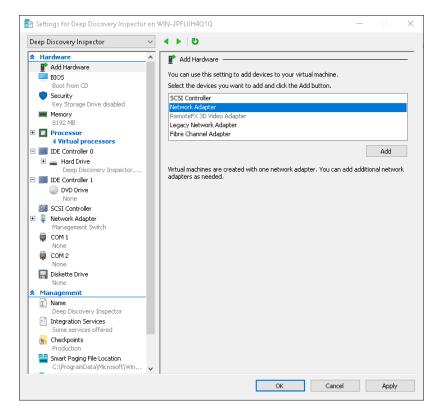
j. For **Media**, select **Image file** and then specify the location of the Deep Discovery Inspector ISO file.



k. In the left column, click Add Hardware.

The Add Hardware settings appear.

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



m. Click Add.

The Network Adapter settings appear.

n. For Virtual switch, select Data Switch.

De	ep Discovery Inspector	\sim	•		G						
*	Hardware	^	Û	Net	twork Adapter						
	📑 Add Hardware			-	the configuration of	the netwo	ek adapt		o the potur	ork ode	otor
	BIOS Boot from CD		L 1		switch:	che necoo	in auapu	a or remov	e the netwo		ipcer.
	Security				Switch				~		
	Key Storage Drive disabled		- v	LAN	ID						
	Memory 8192 MB				Enable virtual LAN ide	ntification					
+	Processor 4 Virtual processors IDE Controller 0 Hard Drive				VLAN identifier specif vork communications 2				tual machin	e will u:	se for all
F	Deep Discovery Inspector. IDE Controller 1		в	andv	width Management —						
	DVD Drive None				Enable bandwidth ma	-					
	SCSI Controller				cify how this network dwidth and Maximum						
ŧ	Network Adapter Management Switch			Minin	mum handwidth:		0	Mbps			
+	Network Adapter						-				
	Data Switch		'	Maxi	imum bandwidth:		0	Mbps			
	COM 1 None			0	To leave the minimum	n or maxim	num unre	stricted, sp	ecify 0 as th	ne valu	е,
	COM 2 None		То	remo	ove the network ada	oter from t	his virtua	al machine,	click Remov	e.	
	🔜 Diskette Drive										Remove
	None			Us	se a legacy network a	dapter ins	tead of t	his network	adapter to	perfor	ma
^	Management Name	- 11		ne	etwork-based installat ervices are not installe	ion of the	guest op	erating sys	tem or whe		
	Deep Discovery Inspector			58	a vices are flut il istalit	sa in che gi	aesc oper	aung syste	an.		
	Integration Services Some services offered										
	Checkpoints Production										

- o. Click Apply.
- p. Click OK.
- 5. Configure the Hyper-V network for mirroring.

For details, see *Configuring internal VM traffic mirroring in Microsoft Hyper-V on page 7-39* and *Configuring external traffic mirroring in Microsoft Hyper-V on page 7-37*.

Configure traffic mirroring in Microsoft Hyper-V

Learn how to enable the capture of external and internal VM traffic in the following topics:

- Configuring external traffic mirroring in Microsoft Hyper-V on page 7-37
- Configuring internal VM traffic mirroring in Microsoft Hyper-V on page 7-39

Configuring external traffic mirroring in Microsoft Hyper-V

Perform the follow steps on the Deep Discovery Inspector host to enable the capture of external mirrored traffic.

Procedure

1. On the Hyper-V host, run the following commands in Powershell to configure the monitor mode of the Data Switch.

```
$DataSwitch = "Data Switch"
$extFeature = Get-VMSystemSwitchExtensionPortFeature `
    -FeatureName "Ethernet Switch Port Security Settings"
$extFeature.SettingData.MonitorMode = 2
Add-VMSwitchExtensionPortFeature `
    -ExternalPort -SwitchName $DataSwitch `
    -VMSwitchExtensionFeature $extFeature
```

2. Run the following commands in Powershell to verify that the settings are configured correctly.

```
$extFeature = Get-VMSwitchExtensionPortFeature `
    -ExternalPort -SwitchName $DataSwitch `
    -FeatureName "Ethernet Switch Port Security Settings"
$extFeature.SettingData.MonitorMode
```

If configured correctly, the resulting output is **2** to indicate that the port mirroring mode is **source**.

- 3. Configure the monitor mode of the VM Network Adapter.
 - **a.** In Hyper-V Manager, click on the Deep Discovery Inspector VM and then go to **Action** > **Settings**.

The settings window appears.

b. Expand Data Switch and then click Advanced Features.

eep Discovery Inspector	v < <p>♦</p>	
tardware	Enable MAC address spooting	
📑 Add Hardware		
🛑 BIOS	DHCP guard	
Boot from CD	DHCP guard drops DHCP server messages from unauthorized virtual ma	chines
💙 Security	pretending to be DHCP servers.	
Key Storage Drive disabled	Enable DHCP guard	
Memory		
32768 MB	Router guard	
Processor I Virtual processor	Router guard drops router advertisement and redirection messages from	m
IDE Controller 0	unauthorized virtual machines pretending to be routers.	
IDE Controller U IDE Controller U	Enable router advertisement guard	
 Hard Drive Deep Discovery Inspector. 		
IDE Controller 1	Protected network	
DVD Drive	Move this virtual machine to another cluster node if a network disconner	stion is
DeepDiscoveryInspector_I	detected.	cuorris
🗐 SCSI Controller	Protected network	
🗉 🃮 Network Adapter		
Management Switch		
🖃 📮 Network Adapter	Port mirroring	
Data Switch	Port mirroring allows the network traffic of a virtual machine to be monit copying incoming and outgoing packets and forwarding the copies to an	
Hardware Acceleration	virtual machine configured for monitoring.	04101
Advanced Features	Mirroring mode:	
💭 COM 1	None	
None	Destination	
COM 2	NIC Teaming Source	
Diskette Drive	You can establish NIC Teaming in the guest operating system to aggreg. bandwidth and provide redundancy. This is useful if teaming is not confi	
None	the management operating system.	garca In
* Management	Enable this network adapter to be part of a team in the guest opera	atina
1 Name	system	
Deep Discovery Inspector	When this option is cleared, a team created in the quest operating syste	em will
📄 Integration Services	lose connectivity if one of the physical network adapters stops working.	
Some services offered	v	

c. For Mirroring mode, select Destination.

d. Click OK.

4. Run the following commands in Powershell to configure the VLAN mode of the Data Switch.

```
$VMName = "Deep Discovery Inspector"
$DataSwitch = "Data Switch"
Get-VMNetworkAdapter -VMName $VMName |
? SwitchName -eq "$DataSwitch" |
```

```
% { Set-VMNetworkAdapterVlan -VMNetworkAdapter $_ `
-Trunk -AllowedVlanIdList 1-4094 -NativeVlanId 0 }
```

5. (Optional) Run the following commands in Powershell to configure the jumbo MTU setting on the physical adapter and prevent dropped network packets.

🖉 Note

For the \$NetAdapter value, use the name of the physical network adapater on the Hyper-V host.

```
$NetAdapter = "Ethernet0"
Get-NetAdapterAdvancedProperty -Name $NetAdapter `
-RegistryKeyword "*jumbopacket" |
Set-NetAdapterAdvancedProperty -RegistryValue 4088
```

6. Start the virtual machine and verify that the traffic is mirrored and detected.

Configuring internal VM traffic mirroring in Microsoft Hyper-V

Perform the follow steps on the Deep Discovery Inspector host to enable the capture of mirrored traffic from a VM on the same host.

Procedure

 In Hyper-V Manager, click on the Deep Discovery Inspector virtual machine and then go to Action > Settings.

The settings window appears.

2. In the left column, click Add Hardware.

The Add Hardware settings appear.

- 3. For the devices you want to add, select Network Adapter.
- 4. Click Add.

The Network Adapter settings appear.

- 5. For Virtual switch, select Management Switch.
- 6. In the left column, expand **Management Switch** and then click **Advanced Features**.
- 7. For Mirroring mode, select Destination.
- 8. Click OK.
- **9.** In Hyper-V Manager, click on the virtual machine that is on the same host as Deep Discovery Inspector and then go to **Action** > **Settings**.

The settings window appears.

- **10.** In the left column, expand **Management Switch** and then click **Advanced Features**.
- 11. For Mirroring mode, select Source.
- 12. Click OK.

7-40

13. Start the Deep Discovery Inspector virtual machine and verify that the traffic is mirrored and detected.



Chapter 8

Installation on a virtual appliance

Learn the steps for installing Deep Discovery Inspector as a virtual appliance in the following sections.



Configuring options

Set the following options to enable Deep Discovery Inspector management console navigation.

- Setting JavaScript options for Google Chrome on page 8-2
- Setting JavaScript options for Mozilla Firefox on page 8-2
- Setting options for virtual appliance in ESXi on page 8-3

Setting JavaScript options for Google Chrome

Procedure

- 1. On the browser, go to **Settings**.
- 2. Click Show advanced settings....
- 3. Under Privacy, click Content settings....
- 4. Under JavaScript, click Allow all sites to run JavaScript (recommended).
- 5. Click Done.

Setting JavaScript options for Mozilla Firefox

Procedure

- 1. For Firefox versions lower than 23, do the following.
 - **a.** On the browser, go to the **Options** > **Content** tab.
 - **b.** Verify that **Enable JavaScript** is selected.
 - c. Click OK.
- 2. For Firefox version 23 or higher, do the following.
 - a. In the address bar, type about: config and press ENTER.

- b. Click I'll be careful, I promise!.
- **c.** Verify that the **Value** of **Preference Name javascript.enabled** is set to **true**.

Setting options for virtual appliance in ESXi

The following steps apply to the supported versions of ESXi. For details, see *Requirements for a virtual machine in VMware ESXi on page 7-2*.

Procedure

1. Go toVMware 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.

- VMware Tools			ŕ
Power Operations	Shut Down Guest	~	
	Put Guest on Standby	~	
	Power On / Resume VM		
	S Restart Guest	~	
Run VMware Tools Scripts	 ✓ After powering on ✓ After resuming ✓ Before suspending ✓ Before shutting down guest 		
Tools Upgrades	Check and upgrade VMware Tools before each power on		
Time	Synchronize guest time with host		
Power management	Expand for power management settings		
	man and a second s		l

Deep Discovery Inspector virtual appliance installation

You can install Deep Discovery Inspector on:

• VMware ESXi 7.0 or 8.0.

You must obtain a separate license for VMware ESXi. Your usage is subject to the terms and conditions outlined in the VMware license agreement specific to that product.

- Microsoft Hyper-V on Windows Server 2019 or 2022.
- KVM.

Procedure

1. Back up any pre-existing data on the target hard drive before installing Deep Discovery Inspector.

The installation process formats and repartitions the hard drive and removes all existing data.

If you are reinstalling Deep Discovery Inspector, you can back up your current settings by going to **Administration** > **System Maintenance** > **Backup / Restore** in the Deep Discovery Inspector management console.

2. Create a virtual appliance.

Tip

For details, see Create a new virtual appliance on page 7-1.

When installing Deep Discovery Inspector on a VMware ESXi server, disable the snapshot feature for the virtual appliance to preserve hard disk space.

3. Start the virtual machine.

8-4

4. Insert the Deep Discovery Inspector installation DVD into the physical CD/DVD drive of the hypervisor server.

- **5.** Connect the virtual CD/DVD drive of the virtual appliance to the physical CD/DVD drive of the hypervisor server.
- 6. Connect the virtual CD/DVD drive of the virtual appliance to the ISO file.
- 7. Restart the virtual appliance.
 - In the VMware vSphere Client, go to Inventory > Virtual Machine > Guest > Send and press CTRL + ALT + DEL.
 - On the KVM server, use a management tool.

For details, see <u>https://www.linux-kvm.org/page/</u> <u>Management_Tools</u>.

• In the Hyper-V Manager, select the server, shut down the server, and start the server.

The Installation DVD screen appears.

```
Trend Micro Deep Discovery Inspector
Installation DUD
Welcome to Deep Discovery Inspector
(1) Start the installation process
(2) Automatically evaluate and mirror network environment setup.
Type a number and press [ENTER].
The installation proceeds with the default option (1) if there is no option
chosen after 15 seconds.
```

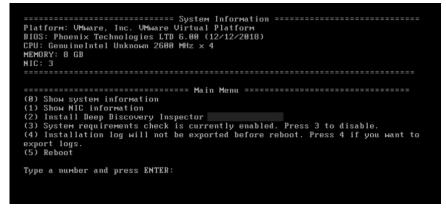
8. Press ENTER.



Important

When installing Deep Discovery Inspector through a serial connection, type serial and press ENTER

The System Information screen appears.



9. For trial deployments, type **3** and press **ENTER** to skip the system requirements check.



8-6

By default, the installer checks system requirements before installing Deep Discovery Inspector to confirm that the appliance has the necessary resources to run the product.

- **10.** If you need to obtain installation logs for troubleshooting, type **4** and press ENTER.
- 11. Start the installation by typing 2 and pressing ENTER.

The Management Port Selection screen appears.

Deep Discovery Inspector automatically detects the active link cards (indicated by Link UP) available for use as a management port.

-Management Port Selection Select an active link card to use for the management port. If unsure which one is connected to your management domains 1. Disconnect all network cables. 2. Select cardinates the context of the select			
JnBoard Port 1 JnBoard Port 3 JnBoard Port 3 JnBoard Port 4 Jot 7 Port 1 Jot 7 Port 2 Jot 4 Port 2 Jot 1 Port 2	Link UF , Intel Corporation 1350 Gigabit Network Connecti Link DUMM, Intel Corporation 1350 Gigabit Network Connecti Link DUMM, Intel Corporation 3350 Gigabit Network Connecti Link DUMM, Intel Corporation 3350 Gigabit Network Connecti Link DUMM, Intel Corporation 3550 Gigabit Network Connecti Link DUMM, Intel Corporation Ethernet Controller X710 for) 71z-71z		
	< OK > <re-detect></re-detect>		

FIGURE 8-1. Management Port Selection

12. Verify that the network port status and the actual port status match.

If a status conflict exists, select Re-detect and press ENTER.

- **13.** Check which active link card connects to the management domain by doing the steps listed on the **Management Port Selection** screen.
- 14. Select an active link card and press ENTER.

The installation continues and completes.

- **15.** If you enabled installation log export on the **System Information** screen, save the installation logs.
 - **a.** Select a storage device and press ENTER.

If your storage device is not listed, Go to **Re-detect** and press **ENTER** to refresh the list.

b. When the installation log file name appears, press ENTER.

Record the file name for future reference. The file name uses the following format:

install.log.YYYY-MM-DD-hh-mm-ss

Tip Trend Micro recommends saving exported installation logs to sda11.

The system automatically restarts and the Preconfiguration Console appears. If used, the installation DVD ejects from the CD/DVD drive.

- 16. (Optional) Remove the DVD to prevent reinstallation.
- 17. Configure the Deep Discovery Inspector network settings.
 - Access the preconfiguration console and change the device settings.

For details, see Preconfiguration on page 10-1.

• Open the management console and change the appliance IP settings.

For details, see the *Get Started* chapter of the *Deep Discovery Inspector Administrator's Guide*.

What to do next

8-8

See the *Deep Discovery Inspector Administrator's Guide* for details about configuring and administering Deep Discovery Inspector.



Chapter 9

Port mirroring on a VMware virtual distributed switch

Deep Discovery Inspector can monitor mirrored traffic using virtual distributed switches. Learn how to create a virtual distributed switch and configure Deep Discovery Inspector virtual appliances to monitor mirrored traffic in the following sections.

- Creating a VMware vSphere distributed switch (VDS) on page 9-2
- Deep discovery inspector virtual appliance with a VDS on page 9-5

Creating a VMware vSphere distributed switch (VDS)

Procedure

- 1. Create a new virtual distributed switch.
 - **a.** Log in to the vSphere Web Client.
 - b. Click Networking.
 - c. In the left panel, select your data center.
 - d. In the right panel, click the Create a new distributed switch icon.The New Distributed Switch window appears.
 - e. Type a name for the switch and then click Next.
 - f. Select the distributed switch version and then click **Next**.
 - **g.** For **Number of uplinks**, set at least **2** if your SPAN traffic is on a dedicated NIC. Otherwise, set this value to **1**.



Trend Micro recommends using a dedicated NIC.

- h. For Network I/O Control, select one of the following options.
 - **Disabled**: If your SPAN traffic on a dedicated NIC.



Trend Micro recommends using a dedicated NIC.

- **Enabled**: If your SPAN traffic is on the same NIC as your monitored traffic.
- i. Uncheck Create a default port group.
- j. Click Next.

9-2

- **k.** Verify that the summary information is correct and then click **Finish**.
- 2. Configure the virtual switch.
 - **a.** Right-click the virtual distributed switch you created in the previous steps, and then select **Settings** > **Edit Settings**.

The Edit Settings window appears.

b. Click Advanced.

The advanced settings appear.

- c. For MTU (Bytes), specify 1600.
- 3. Add port groups to the virtual distributed switch.
 - a. Click Networking.
 - b. Right-click the virtual distributed switch you created in the previous steps, and then select Distributed Port Group > New Distributed Port Group.

The New Distributed Port Group window appears.

- **c.** Type a name for the port group and then click **Next**.
- d. For Port binding, select Static binding.
- e. For Port allocation, select Fixed.
- **f.** For **Number of ports**, type the number of ports that you want to connect.
- g. Click Next.
- **h.** Verify that the settings on the summary screen are correct and then click **Finish**.

The new port group appears on the Manage tab.

- 4. (Optional) Repeat step 3 to add additional port groups.
- 5. Add an ESXi host to the virtual distributed switch.

a. Right-click the virtual switch you created in the previous steps, and then select **Add and Manage Hosts**.

The Add and Manage Hosts window appears.

- **b.** For Select task, select Add host and manage host networking (advanced).
- c. Click Next.
- d. For Select hosts, click + New hosts to add managed ESXi hosts.
- e. Click Next.
- f. For Selet network adapter tasks, add a checkmark to Manage physical adapters and Migrate virtual machine networking.
- g. Click Next.
- **h.** For **Manage physical network adapters**, manage the physical network adapters according to your network environment.
- i. Click Next.
- j. For Analyze impact, specify No impact.
- k. Click Next.
- **1.** For **Migrate VM networking**, migrate the VM networking according to your network environment.
- m. Click Next.
- n. For Ready to complete, click Finish.

The Add and Manage Hosts window closes.

o. Click the virtual switch you created in the previous steps, click the **Configure** tab, and then click **Topology** to verify the virtual switch topology that you configured.

Deep discovery inspector virtual appliance with a VDS

Deep Discovery Inspector virtual appliances can monitor mirrored virtual distributed switch traffic that is inside and outside virtual environments. Learn about the requirments and how to configure Deep Discovery Inspector and the virtual distrbuted switch in the following sections.

- Requirements for virtual appliances with a VDS on page 9-5
- Virtual appliance monitoring mirrored external network traffic using a VDS on page 9-7
- Virtual appliance monitoring mirrored VM traffic from a VDS on page 9-14

Requirements for virtual appliances with a VDS

The following table describes the minimum physical NIC requirements for Deep Discovery Inspector virtual appliances.

TRAFFIC SOURCE	Remote Mirroring	Encapsulated Remote Mirroring	DISTRIBUTED PORT MIRRORING
External network traffic	The destination ESXi host requires a 1 Gbps Ethernet network port as an uplink	The destination ESXi host requires a 1 Gbps Ethernet network port as an uplink Note The port must be routable from the enscapsulate d remote mirroring source.	Not supported
VM network traffic	Each ESXi host requires a 1 Gbps Ethernet network port as an uplink	The destination ESXi host requires a 1 Gbps Ethernet network port as an uplink Note The port must be routable from the other ESXi host management VMkernel port.	No physical port requirement

TABLE 9-1. Virtual Appliance Physical NIC Requirements

9-6

Virtual appliance - monitoring mirrored external network traffic using a VDS

Deep Discovery Inspector virtual appliances can monitor mirrored traffic using a virtual distributed switch with encapsulated remote mirroring or remote mirroring. Learn how to configure Deep Discovery Inspector and the network devices in the following sections.

- Virtual appliance configuring mirrored external network traffic monitoring with encapsulated remote mirroring on page 9-8
- Virtual appliance configuring mirrored external network traffic monitoring with remote mirroring on page 9-10

Virtual appliance - configuring mirrored external network traffic monitoring with encapsulated remote mirroring

Encapsulated Remote Mirroring enables you to monitor traffic on multiple network interfaces or VLANs and send the monitored traffic to one or more destinations.

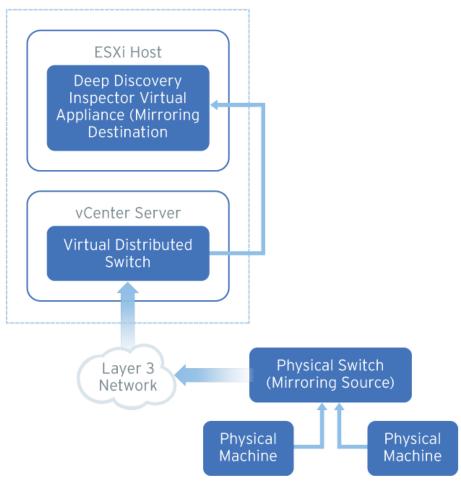


FIGURE 9-1. Mirrored External Network Traffic Monitoring with Encapsulated Remote Mirroring

9-8

By default, encapsulated remote mirroring on the virtual switch uses the management VMkernel port of the ESXi host as the encapsulation source IP address.

In the steps below, the mirroring source and mirroring destination are the following:

- · Mirroring source: Physical switch that forwards mirrored traffic
- Mirroring destination: Deep Discovery Inspector

Procedure

1. Configure the mirroring source to forward encapsulated remote mirrored traffic.



Important

Ensure that switch is able to route traffic to the encapsulated remote mirroring destination IP address that you configure on Deep Discovery Inspector in the next step.

- **2.** Configure the mirroring destination to receive encapsulated remote mirrored traffic.
 - a. In the Deep Discovery Inspector console, go to Administration > System Settings > Network Interface.

The Network Interface screen appears.

b. Locate a data port, and then click the right arrow (

) at the beginning of the row.

- c. Select Encapsulated Remote Mirroring.
- d. Specify the encapsulated remote mirroring destination address.
- e. Click Save.

Virtual appliance - configuring mirrored external network traffic monitoring with remote mirroring

Remote mirroring enables you to monitor traffic on one switch through a device on another switch and send the monitored traffic to one or more destinations.

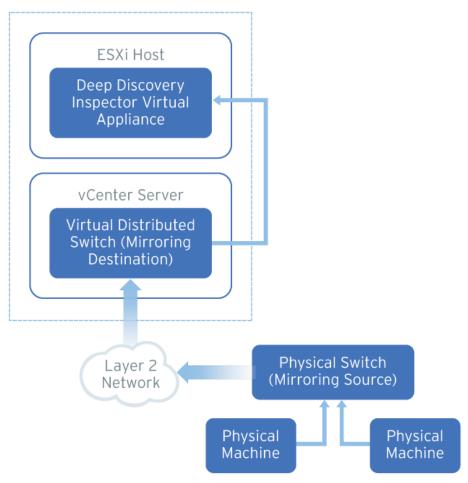


FIGURE 9-2. Mirrored External Network Traffic Monitoring with Remote Mirroring

9-10

9-11

Remote mirroring requires that you configure a remote mirroring VLAN on your physical switches. If you cannot configure a remote mirroring VLAN, consider using encapsulated remote mirroring as an alternative.

In the steps below, the mirroring source and mirroring destination are the following:

- Mirroring source: Physical switch that forwards mirrored traffic to the virtual distributed switch
- Mirroring destination: Virtual distributed switch that recieves mirrored traffic

Before you begin, verify that the uplink ports of the ESXi hosts that receive traffic are linked to the physical switch trunk port.

Procedure

- **1.** Configure the mirroring source to forward mirrored traffic to the mirroring destination.
- 2. Configure the mirroring destination recieve mirrored traffic.
 - a. Log in to the vSphere Web Client.
 - **b.** Select your virtual distributed switch in the left column and then click **Configure**.
 - c. Click Port Mirroring.

The Port mirroring screen appears.

Navigator I	🖙 DSwitch 🛛 🔽 🍰 🕼 🙉 🧔 🛛 🍪 Actions 🗸
Back	Getting Started Summary Monitor Configure Permissions Ports Hosts VMs Networks
Image: Constraint of the state of	H Port mirroring Settings New Properties Session Name Type
VM Network	Topology Session Name Type
Construction	LACP Private VLAN NetFlow Port mirroring Health check • Resource Allocation
	System traffic M Network resource pools
	✓ More Network Protocol Profiles

d. Click New....

The Add Port Mirroring Sessions window appears.

DSwitch - Add Port Mirroring
1 Select session type 2 Edit properties
3 Select sources 4 Select destinations 5 Ready to complete

- e. Select Remote Mirroring Destination.
- f. Click Next.

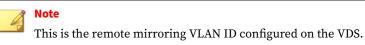
The **Edit properties** screen appears.

Select session type	Edit properties Specify a name and the properties of	of the port mirroring session	
E dit properties Select sources Select destinations Ready to complete	Specify a name and the properties of Name: Status: Session type: Advanced properties Normal VO on destination ports: Mirrored packet length (Bytes): Sampling rate: Description:	f the port mirroring session.	
		Back Next	Canc

- g. In Name, type a session name.
- h. For Status, select Enabled.
- i. Click Next.

The **Select sources** screen appears.

j. Click the plus icon to add the VLAN ID that you want to monitor.



k. Click Next.

The **Select destinations** screen appears.

I. Click the plus icon

(

) to add the port ID of the Deep Discovery Inspector data port.

9 - 13

m. Click Next.

The **Ready to complete** screen appears.

n. Verify that the settings are correct and then click **Finish**.

Virtual appliance - monitoring mirrored VM traffic from a VDS

Deep Discovery Inspector virtual appliances can monitor mirrored traffic from the same ESXi host that contains Deep Discovery Inspector or different ESXi hosts . Learn how to configure Deep Discovery Inspector and the virtual distrbuted switch in the following sections.

- Virtual appliance monitoring mirrored traffic from different ESXi hosts on page 9-14
- Virtual appliance monitoring mirrored traffic from the same ESXi host on page 9-26

Virtual appliance - monitoring mirrored traffic from different ESXi hosts

Deep Discovery Inspector virtual appliances can monitor mirrored VM traffic from a different ESXi hosts using encapsulated remote mirroring or remote mirroring. Learn how to configure Deep Discovery Inspector and the virtual distrbuted switch in the following sections.

- Virtual appliance configuring mirrored VM traffic monitoring with encapsulated remote mirroring on page 9-15
- Virtual appliance configuring mirrored VM traffic monitoring with remote mirroring on page 9-20

9 - 15

Virtual appliance - configuring mirrored VM traffic monitoring with encapsulated remote mirroring

Encapsulated Remote Mirroring enables you to monitor traffic on multiple network interfaces or VLANs and send the monitored traffic to one or more destinations.

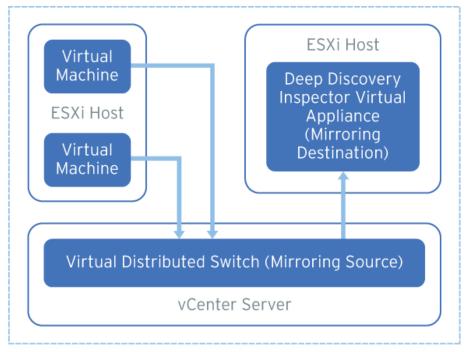


FIGURE 9-3. Mirrored VM Traffic Monitoring with Encapsulated Remote Mirroring

By default, encapsulated remote mirroring on the virtual switch uses the management VMkernel port of the ESXi host as the encapsulation source IP address.

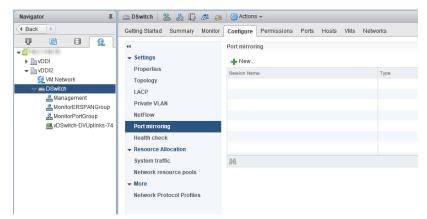
In the steps below, the mirroring source and mirroring destination are the following:

- Mirroring source: Virtual distributed switch that forwards mirrored traffic
- · Mirroring destination: Deep Discovery Inspector

Procedure

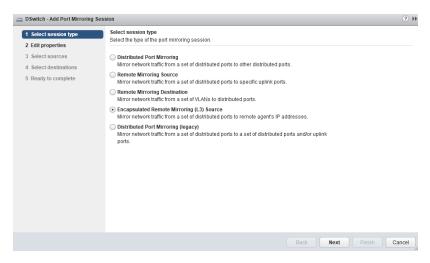
- **1.** Configure the mirroring source to forward encapsulated remote mirrored traffic.
 - **a.** Log in to the vSphere Web Client.
 - **b.** Select your virtual distributed switch in the left column and then click **Configure**.
 - c. Click Port Mirroring.

The **Port mirroring** screen appears.



d. Click New....

The Add Port Mirroring Sessions window appears.



- e. Select Encapsulated Remote Mirroring (L3) Source.
- f. Click Next.

The Edit properties screen appears.

DSwitch - Add Port Mirroring	Session		? H
1 Select session type 2 Edit properties	Edit properties Specify a name and the proper	rties of the port mirroring session.	
 Select sources Select destinations Ready to complete 	Name: Status: Session type: Encapsulation type: Session ID: Advanced properties Mirrored packet length (Bytes Sampling rate: Description:	erspan Enabled • Encapsulated Remote Mirroring (L3) Source GRE • 0	
		Back Next Finish C	

g. In Name, type a session name.

- h. For Status, select Enabled.
- **i.** For **Encapsulation type**, select the encapsulation type.

🛉 Note

Using **ERSPAN THREE** may cause issues. Trend Micro recommends using **GRE** or **ERSPAN TWO**

j. Click Next.

The Select sources screen appears.

k. Click the plus icon

(

1

) to add the source virtual machines that you want to monitor.

I. Click Next.

The **Select destinations** screen appears.

m. Click the plus icon to add an IP address as a destination.

note

The destination IP address is the address that you configure on Deep Discovery Inspector in the next step.

n. Click Next.

The **Ready to complete** screen appears.

- o. Verify that the settings are correct and then click Finish.
- **2.** Configure the mirroring destination to receive encapsulated remote mirrored traffic.
 - a. In the Deep Discovery Inspector console, go to Administration > System Settings > Network Interface.

The **Network Interface** screen appears.

b. Locate a data port, and then click the right arrow (

) at the beginning of the row.

- c. Select Encapsulated Remote Mirroring.
- d. Specify the encapsulated remote mirroring destination address.



Important

The encapsulated remote mirroring destination address must be routable from the management VMkernel port of the ESXi host.

e. Click Save.



Virtual appliance - configuring mirrored VM traffic monitoring with remote mirroring

Remote mirroring enables you to monitor traffic on one switch through a device on another switch and send the monitored traffic to one or more destinations.

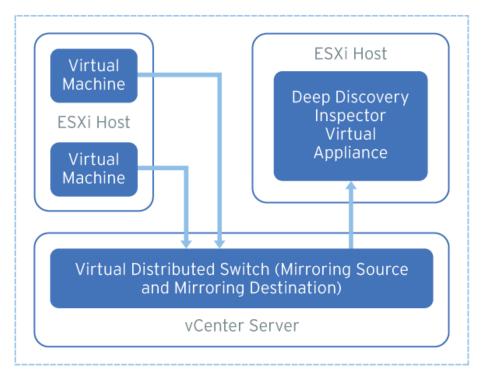


FIGURE 9-4. Mirrored VM Traffic Monitoring with Remote Mirroring

Remote mirroring requires that you configure a remote mirroring VLAN on your physical switches. If you cannot configure a remote mirroring VLAN, consider using encapsulated remote mirroring as an alternative.

In the steps below, the mirroring source and mirroring destination are the following:

9-20

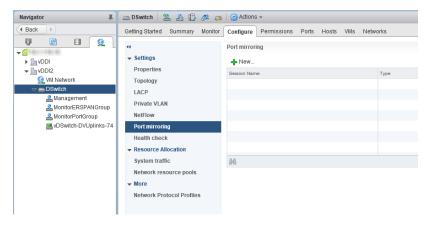
- Mirroring source: Virtual distributed switch that fowards mirrored traffic
- Mirroring destination: Virtual distributed switch that receives mirrored traffic and that can route the traffic to Deep Discovery Inspector

Before you begin, verify that the uplink ports of the ESXi hosts that receive traffic are linked to the physical switch trunk port.

Procedure

- **1.** Configure the mirroring source to forward remote mirrored traffic to the destination.
 - a. Log in to the vSphere Web Client.
 - **b.** Select your virtual distributed switch in the left column and then click **Configure**.
 - c. Click Port Mirroring.

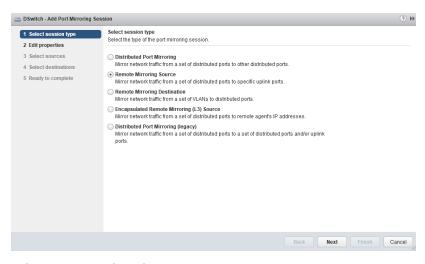
The Port mirroring screen appears.



9-21

d. Click New....

The Add Port Mirroring Sessions window appears.



- e. Select Remote Mirroring Source.
- f. Click Next.

The Edit properties screen appears.

DSwitch - Add Port Mirroring See	ssion	(?) *
 1 Select session type 2 Edit properties 	Edit properties Specify a name and the properties of	the port mirroring session.
 Select sources Select destinations Ready to complete 	, Status: Session type: Encapsulation VLAN ID:	ISPAN Enabled • Remote Mirroring Source 900 • W Preserve original VLAN
	Advanced properties Normal I/O on destination ports: Mirrored packet length (Bytes): Sampling rate: Description:	Disallowed
		Back Next Finish Cancel

g. In Name, type a session name.

- h. For Status, select Enabled.
- i. In Encapsulation VLAN ID, specify the VLAN ID.



This is the remote mirroring VLAN ID configured on the VDS.

j. Click Next.

The Select sources screen appears.

k. Click the plus icon



) to add the source virtual machines that you want to monitor.

I. Click Next.

The Select destinations screen appears.

- m. Add uplink in Available uplinks to Selected uplinks.
- n. Click Next.

The Ready to complete screen appears.

- o. Verify that the settings are correct and then click Finish.
- 2. Configure the mirroring destination to receive mirrored traffic.
 - a. Log in to the vSphere Web Client.
 - **b.** Select your virtual distributed switch in the left column and then click **Configure**.
 - c. Click Port Mirroring.

The Port mirroring screen appears.

Navigator I	🖙 DSwitch 🛛 🔽 🍰 🕼 🙉 🧔 🛛 🍪 Actions 🗸
Back	Getting Started Summary Monitor Configure Permissions Ports Hosts VMs Networks
Image: Constraint of the state of	H Port mirroring Settings New Properties Session Name Type
VM Network	Topology Session Name Type
Construction	LACP Private VLAN NetFlow Port mirroring Health check • Resource Allocation
	System traffic M Network resource pools
	✓ More Network Protocol Profiles

d. Click New....

The Add Port Mirroring Sessions window appears.

DSwitch - Add Port Mirroring Se	Session ?
1 Select session type 2 Edit properties	Select session type Select the type of the port mirroring session.
3 Select sources 4 Select destinations 5 Ready to complete	 Distributed Port Mirroring Mirror network traffic from a set of distributed ports to optical cuplink ports. Remote Mirroring Destination Mirror network traffic from a set of VLANs to distributed ports. Recopsulated Remote Mirroring (L3) Source Mirror network traffic from a set of VLANs to distributed ports to remote agent's IP addresses. Distributed Port Mirroring (Geopcy) Mirror network traffic from a set of distributed ports to a set of distributed ports and/or uplink ports.

- e. Select Remote Mirroring Destination.
- f. Click Next.

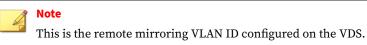
The **Edit properties** screen appears.

DSwitch - Add Port Mirroring	Session		(? H
DSwitch - Add Port Mirroring 1 Select session type 2 Edit properties 3 Select sources 4 Select destinations 5 Ready to complete	Edit properties Specify a name and the properties of Name: Status: Session type: Advanced properties Normal I/O on destination ports:	rspan Enabled • Remote Mirroring Dostination	• • •
	Mirrored packet length (Bytes): Sampling rate: Description:	Enable 60 *	
		Back Next	Finish Cancel

- g. In Name, type a session name.
- h. For Status, select Enabled.
- i. Click Next.

The **Select sources** screen appears.

j. Click the plus icon to add the VLAN ID that you want to monitor.



k. Click Next.

The **Select destinations** screen appears.

I. Click the plus icon

```
*]
```

(

) to add the port ID of the Deep Discovery Inspector data port.

m. Click Next.

9-26

The **Ready to complete** screen appears.

n. Verify that the settings are correct and then click **Finish**.

Virtual appliance - monitoring mirrored traffic from the same ESXi host

Deep Discovery Inspector virtual appliances can monitor mirrored VM traffic from a same ESXi host. Learn how to configure the virtual distrbuted switch in the following section.

• Virtual appliance - configuring distributed port mirroring on a VDS on page 9-27

9-27

Virtual appliance - configuring distributed port mirroring on a VDS

The distributed port mirroring for the virtual distributed switch enables you to monitor traffic from a set of distributed ports to other distributed ports.

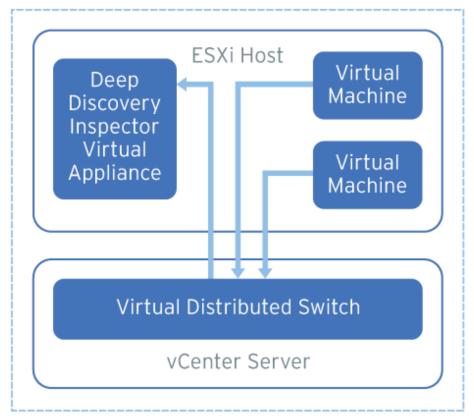


FIGURE 9-5. Distributed Port Mirroring on a VDS

The source virtual machines and destination Deep Discovery Inspector must be on the same ESXi host. If they are on different ESXi hosts, consider using remote mirroring or encapsulated remote mirroring as an alternative.

Procedure

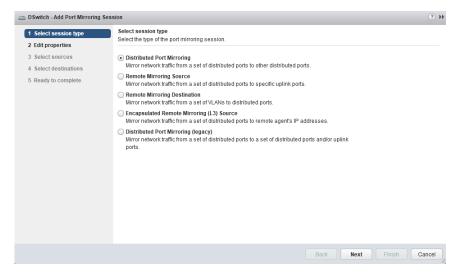
- 1. Log in to the vSphere Web Client.
- 2. Select your virtual distributed switch in the left column and then click **Configure**.
- 3. Click Port Mirroring.

The **Port mirroring** screen appears.

Navigator I	👝 DSwitch 🛛 🔽 🍰 🕼 🚜 🧔 🛛 🤯 Actions 🗸
Back	Getting Started Summary Monitor Configure Permissions Ports Hosts VMs Networks
	Image: Construction of the second
	NELWOIK PIOLOCI PIOLIES

4. Click New....

The Add Port Mirroring Sessions window appears.



- 5. Select Distributed Port Mirroring.
- 6. Click Next.

The **Edit properties** screen appears.

DSwitch - Add Port Mirroring Se	ssion	(?
1 Select session type 2 Edit properties	Edit properties Specify a name and the properties o	the port mirroring session.
3 Select sources 4 Select destinations 5 Ready to complete	Name: Status: Session type: Advanced properties Normal I/O on destination ports: Mirrored packet length (Bytes): Sampling rate: Description:	mirror_port Enabled Distributed Port Mirroring Disallowed Enable 0 1
		Back Next Finish Cancel

9-29

- 7. In Name, type a session name.
- 8. For Status, select Enabled.
- 9. Click Next.

The **Select sources** screen appears.

- 10. Click the plus icon
 - (

†D

) to add the source virtual machines that you want to monitor.

11. Click Next.

The Select destinations screen appears.

12. Click the plus icon

ŧ

) to add the port ID of the Deep Discovery Inspector data port.

13. Click Next.

The **Ready to complete** screen appears.

14. Verify that the settings are correct and then click **Finish**.

Part IV

Post-installation tasks





10-1

Chapter 10

Preconfiguration

Learn how to use the Preconfiguration Console to configure initial Deep Discovery Inspector settings in the following sections:

- Preconfiguration console access on page 10-2
- Preconfiguration console main menu on page 10-4

Preconfiguration console

The Deep Discovery Inspector Preconfiguration Console is a terminal communications program used to configure the network and system settings that are required to access the Deep Discovery Inspector management console.

The Preconfiguration Console also supports recovery operations if the management console is not available.

Use the Preconfiguration Console to do the following:

- Configure initial settings (product IP address and host name)
- Perform a diagnostic test
- Ping the network to verify configuration
- Restart the appliance
- View device information and status
- Change the root password
- · Configure manual traffic bypass

👌 Note

Traffic Bypass is only configurable on supported hardware models.

| Note

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

Preconfiguration console access

The Deep Discovery Inspector Preconfiguration Console is accessible from a hardware or virtual appliance.

Access the Preconfiguration Console as follows:

• Accessing the preconfiguration console with a VGA port on page 10-3

Tip

Trend Micro recommends accessing the Preconfiguration Console using a monitor with a VGA port.

• Accessing the preconfiguration console with a serial port on page 10-3

Accessing the preconfiguration console with a VGA port

Procedure

- 1. Using a VGA cable, connect the monitor VGA port to the appliance VGA port.
- 2. When the Preconfiguration Console screen opens, type the default password admin and press ENTER twice.



Note

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

Accessing the preconfiguration console with a serial port

Procedure

- 1. Using an RS-232 serial cable, connect the serial port of the Deep Discovery Inspector appliance to the serial port on a computer.
- **2.** On the computer, open a serial communication application (HyperTerminal).
- **3.** Type the following values if you are accessing the Preconfiguration Console for the first time:
 - Bits per second: 115200

- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

👔 Note

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

4. When the Preconfiguration Console screen appears, type the default password admin and press ENTER twice.

Preconfiguration console main menu

The Preconfiguration Console main menu displays the following menu items:

TABLE 10-1.	Main Menu Items	
-------------	------------------------	--

Ітем	DESCRIPTION	
1) Device Information and Status	View information about Deep Discovery Inspector and monitor memory usage.	
2) Device Settings	Modify the Deep Discovery Inspector IP address, subnet mask, network default gateway address, and DNS servers.	
3) Interface Settings	View the network speed and duplex mode for the management port, automatically detected by Deep Discovery Inspector.	

10-4

Ітем	DESCRIPTION		
4) System Tasks	 Configure the following: Perform a diagnostic test Ping a server in the same subnet Configure the SSH connection Restart the system Configure manual traffic bypass Note Traffic bypass is only configurable on supported hardware models. 		
5) Change Password	Change the root password.		
6) Log Off with Saving	Log off from the Preconfiguration Console after saving changes.		
7) Log Off without Saving	Log off from the Preconfiguration Console without saving changes.		

To access a menu item, type the number for the menu item and then press ENTER.

Viewing appliance information and status

Use the **Device Information & Status** screen to view the product name, version, and memory usage.

Note

View memory usage information on the Deep Discovery Inspector management console. Go to **Dashboard** > **System Status**.

For details, see *System Status* in the *Deep Discovery Inspector Administrator's Guide*.

Procedure

1. Log on to the Preconfiguration Console.

The Main Menu appears.

2. Type 1 to select Device Information & Status and press ENTER.

📝 Note

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

The Device Information and Status screen appears.

3. Press ENTER to return to the main menu.

Modifying device settings

Use the **Device Settings** screen to configure the management IP address settings.



Note

These tasks can also be performed on the management console.

Procedure

1. Log on to the Preconfiguration Console.

The Main Menu appears.

2. To select Device Settings, type 2 and press ENTER.

👔 Note

To enter data when using a serial communication application (for example, HyperTerminal), disable the scroll lock function on your keyboard. The **Device Settings** screen appears.

- **3.** In the **Type** field, use the space bar to select one of the following properties:
 - dynamic
 - static
- 4. Configure the following IPv4 address settings:
 - a. In the IP address field, type an IPv4 address.

Type a Subnet mask.

- b. Type a Gateway IP address.
- c. Type a **Primary** and **Secondary DNS server** IP address.
- 5. (Optional) Configure the following IPv6 address settings:
 - a. In the Enable field, select yes.
 - **b.** In the **IP address** field, type an IPv6 address.

Type a Subnet prefix.

- c. Type a Gateway IP address.
- d. Type a DNS server IP address.
- **6.** (Optional) Type a VLAN ID.

Note

The VLAN ID is used when a trunk connection is required between the Deep Discovery Inspector management port and a switch. The VLAN ID is used as a VLAN tag in 802.1Q Ethernet frame.

- 7. Go to **Return to main menu** and press ENTER.
- **8.** To save the settings, type 6 and press ENTER.

Modifying interface settings

By default, Deep Discovery Inspector automatically detects the network speed and duplex mode for the management port. These settings may be manually configured.



Note

To maximize throughput, Trend Micro recommends full-duplex mode. Halfduplex is acceptable, but network throughput may be limited by transmission delays.



You can view the network interface settings in the management console. Go to **Administration** > **System Settings** > **Network Interface**. For details, see *Network Interface* in the *Deep Discovery Inspector Administrator's Guide*.

Procedure

1. Log on to the Preconfiguration Console.

The Main Menu appears.

2. Type 3 to select Interface Settings and press ENTER.

note

To enter data when using HyperTerminal, disable the scroll lock function on your keyboard.

The Interface Settings screen appears.

- 3. To change the interface settings, perform the following tasks:
 - **a.** Type **1** and press ENTER.
 - **b.** In the **Speed** and **Duplex** fields, use the space bar to change the network speed and duplex mode.



10-9

- c. Navigate to Return to upper menu and press ENTER.
- 4. Type 2 and press ENTER to return to the main menu.
- **5.** Type **6** and press ENTER to save the settings.



11-1

Chapter 11

System tasks

Learn how to perform system tasks on the Preconfiguration Console in the following topics:

- Performing a diagnostic test on page 11-2
- Performing a ping test on page 11-3
- Restarting Deep Discovery Inspector on page 11-4
- Changing the root password on page 11-4
- Configuring manual traffic bypass on page 11-5
- Logging off on page 11-5

System tasks overview

Use the System Tasks screen to perform the following system tasks.

- Diagnostic test
- Restart system
- Ping test
- SSH Connection
- Traffic Bypass



Traffic Bypass is only displayed on supported hardware models.

Performing a diagnostic test

Run a diagnostic test on Deep Discovery Inspector to capture and view a log of hardware and software status and events.

Procedure

1. Log on to the Preconfiguration Console.

The Main Menu appears.

2. Type 4 and press ENTER.

The System Tasks screen appears.

3. Type **1** and press ENTER.

The **Diagnostic Test** screen appears.

4. On the HyperTerminal console, go to Transfer > Capture Text.

🕜 Note

This step uses HyperTerminal as an example. Other serial communication applications can be used, but this step may be different.

5. Browse to the folder and specify a file name for the log.

🔏 Note

This step uses HyperTerminal as an example. Other serial communication applications can be used, but this step may be different.

6. Click Start.



Note

This step uses HyperTerminal as an example. Other serial communication applications can be used, but this step may be different.

7. Under Run diagnostic test now?, go to OK and press ENTER.

While the diagnostic test runs, Deep Discovery Inspector displays log entries on the console.

After the diagnostic test finishes, Deep Discovery Inspector generates a summary log report, and automatically restarts.

8. After Deep Discovery Inspector restarts, open the log summary report to view the results.

Performing a ping test

Use a Ping test to verify network configuration.

Procedure

1. Log on to the Preconfiguration Console.

The Main Menu appears.

2. Type 4 and press ENTER.

The System Tasks screen appears.

3. Type **3** and press ENTER.

The **Ping Test** screen appears.

4. Input the server IP address and press **Ping**.

Ping test results appear on the screen.

5. Press ESC to return to the main menu.

Restarting Deep Discovery Inspector

To restart Deep Discovery Inspector, access the Preconfiguration Console using a serial communication application (for example, HyperTerminal). Using Deep Discovery Inspector to access the Preconfiguration Console allows you to restart the appliance remotely.

When Deep Discovery Inspector starts, it verifies the integrity of its configuration files. The management console password may reset if the configuration file containing password information is corrupted. If management console logon is unsuccessful when using the preferred password, log on using the default password admin.

Procedure

1. Log on to the Preconfiguration Console.

The Main Menu appears.

2. Type 4 and press ENTER.

The System Tasks screen appears.

3. Type 2 and press ENTER.

The **Restart System** screen appears.

4. On the **Restart System** screen, navigate to **OK** and press ENTER.

Changing the root password

Procedure

1. Log on to the Preconfiguration Console.

The Main Menu appears.

2. Type 5 and press ENTER.

The Change Password screen appears.

- **3.** Type the old and new passwords.
- 4. Confirm the new password.
- **5.** Go to **Return to main menu** and press ENTER to return to the main menu and save the settings.

Logging off

Log off from the Preconfiguration Console with or without saving.

Procedure

- 1. After changing the configuration settings, return to the main menu.
- 2. Select one of the following logoff options:
 - To save the changes, type 6 and press ENTER.
 - To exit without saving the changes, type 7 and press ENTER.
- 3. Navigate to OK and press ENTER.

Configuring manual traffic bypass

Procedure

1. Log on to the Preconfiguration Console.

The Main Menu appears.

2. Type 4 and press ENTER.

The System Tasks screen appears.

3. Type **5** and press ENTER.

The Manual Traffic Bypass screen appears.

4. Select **Disabled** or **Enabled**.

11-6

5. Press ESC to return to the main menu.



12-1

Chapter 12

Troubleshoot

Learn about common troubleshooting options available in Deep Discovery Inspector and find answers to frequently asked questions in the following topics:

- Frequently asked questions (FAQs) on page 12-2
- Troubleshooting on page 12-5

Frequently asked questions (FAQs)

Find answers to frequently asked questions in the following topics.

- FAQs appliance rescue on page 12-2
- FAQs configuration on page 12-3
- FAQs detections on page 12-3
- FAQs installation on page 12-3
- FAQs upgrade on page 12-4
- FAQs virtual analyzer image on page 12-4

FAQs - appliance rescue

How do I rescue the Deep Discovery Inspector appliance?

To rescue the Deep Discovery Inspector appliance, do one of the following:

• Reinstall Deep Discovery Inspector and use the saved or default settings.



Important

All log data is deleted during reinstallation.

• In the management console, go to **Administration** > **Updates** > **Product Updates** > **Sever Packs / Version Upgrade** and install the service pack or version upgrade file (*.R.tar).



Important

The service pack or version upgrade file must be the same version as the installed version.

How do I rescue the Deep Discovery Inspector appliance from unexpected traffic bypass?

To rescue the Deep Discovery Inspector appliance from unexpected traffic bypass, restart the Deep Discovery Inspector applaince. For details, see *Power Off / Restart* in the *Deep Discovery Inspector Administrator's Guide*.

FAQs - configuration

Can I register Deep Discovery Inspector to more than one Apex Central server?

No, you cannot register Deep Discovery Inspector to more than one Apex Central server. For details on registering to an Apex Central server, see *Registering to Apex Central* in the *Deep Discovery Inspector Administrator's Guide*.

FAQs - detections

Why are there no more Virtual Analyzer detections on the widget or the Log Query screen after Deep Discovery Analyzer or TippingPoint Advanced Threat Protection Analyzer reinstalls?

After Deep Discovery Analyzer or TippingPoint Advanced Threat Protection Analyzer reinstalls, the API key changes. Change the API key on the Deep Discovery Inspector management console from **Administration** > **Virtual Analyzer** > **Setup**.

FAQs - installation

Does Deep Discovery Inspector installation disrupt network traffic?

When deployed out-of-band Deep Discovery Inspector does not disrupt network traffic. When deployed out-of-band, Deep Discovery Inspector installation should not disrupt the network traffic because the appliance connects to the mirror port of the switch and not directly to the network.

When deployed inline, Deep Discovery Inspector can disrupt network traffic.

After a fresh installation, Deep Discovery Inspector is unable to obtain a dynamic IP address. What do I do?

Restart the appliance and verify that it is able to obtain an IP address. Next, connect an Ethernet cable from the management port to a known good Ethernet connection and restart the appliance.

FAQs - upgrade

Can I roll back to a previous version after upgrading to Deep Discovery Inspector 6.7 SP1?

No. The rollback function is not supported.

Why does Deep Discovery Inspector still use old components after updating the software and restarting?

When updating components, Deep Discovery Inspector updates the software first. Restart Deep Discovery Inspector and update the Network Content Inspection Engine. After updating the Network Content Inspection Engine, click **Update**, or wait for the next scheduled update.

How do I verify that the migration was successful?

After the upgrade, go to **Administration** > **System Logs** and in the **Description** column, find the 2 events that are similar to "Attempted to upgrade database instance" and "Updating Deep Discovery Inspector from <old version> to <new version>." Verify that the **Outcome** is **Success** for those 2 events.

What does Deep Discovery Inspector do when the database upgrade process is unsuccessful?

Deep Discovery Inspector rebuilds a new, empty database. All previous database data is not recoverable.

FAQs - virtual analyzer image

I am unable to download images from an FTP server. What should I do?

Verify the following:

- The specified server path, user name, and password are correct
- · Both active and passive modes are enabled on the FTP server
- The FTP server supports UTF-8 (in case image names or file paths contain multi-byte characters)

The Found New Hardware wizard opens when the image is tested in VirtualBox. Does this affect Virtual Analyzer?

The **Found New Hardware** wizard automatically runs whenever an image is transferred from one machine to another. If the **Found New Hardware** wizard appears when the image is tested in VirtualBox, it may interfere with the CD/DVD auto-run.

Troubleshooting

This section describes common troubleshooting options available in Deep Discovery Inspector.

- Slow management console response on page 12-5
- Detections on page 12-6
- "database is corrupt" alert displays on page 12-8
- Virtual analyzer on page 12-8
- Virtual analyzer images on page 12-9
- Cannot connect to network services on page 12-11
- Diagnostics on page 12-11

Slow management console response

The management console response is slow or times out.

This occurs when system resources are insufficient.

Procedure

- To verify CPU, memory, and disk usage, go to https://<appliance IP address>/html/troubleshooting.htm.
- 2. Under Real-time Status, select System Process (ATOP).

The System Process screen appears.

3. Click Suspend and verify system resources real-time.

Ітем	LINE	COLUMN	DESCRIPTION
CPU	CPU	Idle	The lower the number, the busier the CPU is. If this number is low, view the process information and record the CPU with the highest usage.
МЕМ	МЕМ	Free, cache	The "Free" field indicates available memory. A low number means that there is not enough available memory to complete certain actions.
Disk	DSK	Busy	A high number indicates that the disk is busy.

TABLE 12-1. System Resources

Detections

- No detections on all detections screen on page 12-6
- "unregistered service" server displays in all detections query on page 12-7
- Unknown IP addresses display on a screen on page 12-7
- Known safe objects flagged as malicious on page 12-7

No detections on all detections screen

No detections appear on the management console All Detections screen.

Procedure

1. Verify that the switch mirror port is configured to mirror both directions of network traffic to the mirror port.

For details, see *Deployment Planning* in the *Deep Discovery Inspector Installation and Deployment Guide.*

- 2. Verify that networked packets can be captured.
 - a. Go to the troubleshooting pages at https://<appliance IP address>/html/troubleshooting.htm and then click on Network Traffic Dump.

- **b.** In the drop-down menu, select the data port in use.
- c. Click Capture Packets.
- d. Wait 10 seconds and click Stop.
- e. Click View.

The Packet Capture Information screen appears.

- 1. In the **Capfile information** section, verify that the data rate matches the real-time traffic rate.
- 2. Click **Conversation by TCP** or **Conversation by UDP**, and verify that TCP and UDP packets are visible.

"unregistered service" server displays in all detections query

A server appears as an **Unregistered service** on the **All Detections** screen.

Verify that the server has been added to the Registered Services list. For more details, see *Adding Registered Services* in the *Deep Discovery Inspector Administrator's Guide*.

Unknown IP addresses display on a screen

IP addresses that do not belong to your network appear on a screen.

Make sure that all IP addresses in your network have been added to the network group correctly. For details, see *Adding Network Groups* in the *Deep Discovery Inspector Adminstrator's Guide*.

Known safe objects flagged as malicious

Known safe files, IP addresses, domains, and URLs are flagged malicious by Virtual Analyzer.

• Add any safe objects to the Allow List. For details, see *Creating a Custom Allow List* in the *Deep Discovery Inspector Administrator's Guide*.

• Move any safe objects from the Suspicious Objects list to the Allow List. For details, see *Viewing Suspicious Objects* in the *Deep Discovery Inspector Administrator's Guide*.

"database is corrupt" alert displays

The management console displays the "Database is corrupt" alert.

This message occurs when the database has been corrupted. As a precaution, data is not written to the database, which now must be manually repaired. For details, see *Performing Product Database Maintenance* in the *Deep Discovery Inspector Administrator's Guide*.



WARNING!

Performing manual repairs on a database results in permanent loss of data.

Virtual analyzer

- Cannot upload OVA on page 12-8
- No virtual analyzer response to file submissions on page 12-8

Cannot upload OVA

The OVA is too large and cannot upload into Deep Discovery Inspector.

The OVA image must be between 1 GB and 30 GB in size.

No virtual analyzer response to file submissions

File samples were sent to Deep Discovery Inspector but no response was received from Virtual Analyzer.

To receive results, enable file submission to Virtual Analyzer.

Procedure

1. Verify that Virtual Analyzer is enabled.

For details, see Enabling Virtual Analyzer in the Deep Discovery Inspector Administrator's Guide.

- 2. Go to Administration > Virtual Analyzer > File Submissions > Add and verify file submission rules are configured as follows:
 - Under Criteria, click the applicable file types.
 - Under Actions, click Submit.

For details, see *File Submission Rules* in the *Deep Discovery Inspector Administrator's Guide*.

- 3. Go to Dashboard > Virtual Analyzer Status and view the Virtual Analyzer status field on the Virtual Analyzer widget.
 - a. If Virtual Analyzer status is "Disabled", enable Virtual Analyzer. Go to Administration > Virtual Analyzer > Setup to enable file submission to a Virtual Analyzer.

For details, see *Enabling Virtual Analyzer* in the *Deep Discovery Inspector Administrator's Guide*.

- **b.** If the Virtual Analyzer status is "Enabled", restart Deep Discovery Inspector.
- 4. Verify notification settings.

For details, see *Configuring Email Notification Settings* in the *Deep Discovery Inspector Administrator's Guide*.

5. If the problem persists, contact your technical support provider.

Virtual analyzer images

- The installation media does not start on page 12-9
- "found new hardware" wizard on page 12-10
- An image displays a blue screen on page 12-10

The installation media does not start

The installation CD/DVD does not automatically start.

Verify items by testing the Virtual Analyzer images in VirtualBox.

Procedure

- 1. In Oracle VM VirtualBox Manager, click the imported custom Virtual Analyzer image in the left panel.
- 2. Click Settings and select Storage.
- 3. Select **Controller: IDE** and verify that the specified type is **PIIX4**.
- 4. Select the optical disc icon and verify that the specified CD/DVD drive is **IDE Secondary Master**.

"found new hardware" wizard

During Virtual Analyzer image creation, the **Found New Hardware** wizard appears.

The **Found New Hardware** wizard automatically runs whenever an image is transferred from one machine to another.

When an image is imported, the **Found New Hardware** wizard may interfere with the CD/DVD auto-run. Make sure the Virtual Analyzer image is created and prepared using the correct procedure. For details, see the *Virtual Analyzer Image Preparation User's Guide* at <u>https://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx</u>.

An image displays a blue screen

An image displays the blue "Cannot find Operating System" screen when tested in VirtualBox.

Verify items by testing the Virtual Analyzer images in VirtualBox.

Procedure

1. In Oracle VM VirtualBox Manager, click the imported custom Virtual Analyzer image in the left panel.

- 2. Click the Settings and select System.
- 3. On the Motherboard tab, verify that the following are selected:
 - Chipset: ICH9
 - Enable IO APIC
- 4. On the **Processor** tab, verify that the PAE/NX is enabled.
- 5. On the Acceleration tab, verify that the TV-x/AMD-V is enabled.

Cannot connect to network services

You can use the **Network Services Diagnostics** screen to test the network connections for the internal Virtual Analyzer and other network services.

Procedure

- Go to https://<appliance IP address>/html/troubleshooting.htm and click Network Services Diagnostics.
- 2. Select one or more enabled services and click Test.

Wait for the connection test to complete. The time required depends on the network environment and the number of services selected. View the connection test result in the **Result** column.

Diagnostics

For any issue not mentioned, run diagnostics to give test results and debug logs to your Trend Micro Deep Discovery Inspector support provider.

Procedure

- **1.** Open the preconfiguration console.
- 2. Select 4) System Tasks, and press ENTER.
- **3.** Follow the instructions in *Performing a Diagnostic Test* in the *Deep Discovery Inspector Installation and Deployment Guide*.

12-11

- 4. Generate a debug log.
 - a. Go to https://<appliance IP address>/html/ troubleshooting.htm.
 - **b.** Go to **Logs** > **Debug Logs**
 - **c.** Under **Debug Log Settings**, set the debug level to **Debug** for the modules you want to debug.

To avoid performance loss, only set the debug level to **Debug** for required modules. Contact your support provider for advice on how to set the level to debug and obtain the debug report.

- d. Click Save.
- e. If possible, reproduce the issue.
- f. Select one or more debug logs to export.
 - Export debug log.
 - · Export advanced debug log.
 - Select one or more dated debug logs under **Export advanced debug log** to export the advanced debug log for that date.
- g. Click Export.

) Tip

To conserve system resources, perform one export at a time.

- h. Under Debug Log Settings, click Reset to default log settings.
- i. Under Debug Log Maintenance, click Purge Debug Logs.

Inline deployment and TLS inspection

- Network connectivity issue on page 12-13
- TLS connection issue on page 12-14

Network connectivity issue

Procedure

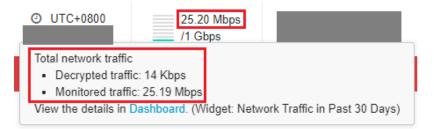
- 1. Verify that the link status of the inline port is connected.
 - a. In the management console, go to Administration > System Settings > Network Interface.
 - **b.** In the **Inline Interfaces** section, view the connection status in the **Status** column.

Click the right arrow () at the beginning of the row to display additional information about the connection status.

Inline Interfaces Inline Interfaces provide uninterrupted network access when traffic can no longer flow through an interface. The Institute namual traffic bypass						
Mode						Collapse All
Inline		Status	Interface		Function	
$ \rightarrow$	•	14	Port 6		Inline traffic	
	Network interface:			Slot 4: Port 1		
		MAC address:		00:e0:ed:da:ff:b7		
	Speed:			Not connected		
	•	si.	Port 7		Inline traffic	
	Network interface: MAC address: Spred:		irface:	Slot 4: Port 2		
			15:	00:e0:ed:da:ff:b8		
				Not connected		

- **2.** If the link status of the inline port is not connected, then verify that the following applicable items are correct.
 - Interface speed setting
 - Interface duplex setting
 - Interface and transceiver compatibility (particularly for fiber connections)
- **3.** Verify that the there is network activity.

a. In the top-right corner of the management console, hover over the throughput to get more information about the network activity.



- 4. If there is no network activity, then verify that TLS traffic inspection is enabled in Deep Discovery Inspector and verify that the cable is securely connected to Deep Discovery Inspector and the network device.
- **5.** (Optional) To monitor when traffic bypass unexpectedly occurs, configure agent mode or trap mode for SNMP in Deep Discovery Inspector.

For details, see Network Interface and SNMP in the Administrator's Guide.

TLS connection issue

Procedure

- 1. Identify the reason for the TLS connection issue.
 - a. In the management console, go to Administration > Monitoring / Scanning > TLS Traffic Inspection > Inspection Settings > Domain Tunneling > Configure tunneled domain.
 - **b.** If you understand and are able to resolve the issue, then do so. Otherwise, use the steps below to continue troubleshooting.
- 2. If you are unable to find the issue in **Domain Tunneling**, then view abnormal connection information in the **TLS Connection Monitoring** troubleshooting screen.

a. Go to https://<appliance IP address>/html/ troubleshooting.htm and then click TLS Connection Monitoring.

The TLS Connection Monitoring screen appears.

- **b.** Type a client IP address and then click **Monitor**.
- c. After sufficient data is monitored, stop the monitoring.



The monitoring can only save up to 10 minutes of data.

- **d.** If you understand and are able to resolve the issue, then do so. Otherwise, use the steps below to continue troubleshooting.
- **3.** If you are unable to find the issue in **TLS Connection Monitoring**, then collect more details and contact your support provider.
 - a. Go to https://<appliance IP address>/html/ troubleshooting.htm and then click TLS Network Traffic Dump.

The TLS Network Traffic Dump screen appears.

- **b.** Type a client IP address and optionally type the server IP address and port, and then click **Capture Packets**.
- c. After sufficient data is captured, stop the capture.
- **d.** If the client application that you are using has a log file with TLS connection information, take a screen shot of the client application log.
- e. Take screen shots of your TLS traffic inspection settings.
- **f.** Send the traffic dump and screen shots to your support representative.

Part V

Technical support

Learn about the following topics:

- Troubleshooting resources on page 13-1
- Contacting Trend Micro on page 14-1
- Sending suspicious content to Trend Micro on page 15-1
- Other resources on page 16-1



13-1

Chapter 13

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.
- 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/smb-new-request

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

Threat encyclopedia

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

Go to <u>https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware</u> to learn more about:

· Malware and malicious mobile code currently active or "in the wild"

- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports





Chapter 14

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:

14-1

https://docs.trendmicro.com



14 - 3

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



15-1

Chapter 15

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://servicecentral.trendmicro.com/en-us/ers/

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

https://success.trendmicro.com/solution/1112106

File Reputation Services

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

https://success.trendmicro.com/solution/1059565

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):

https://global.sitesafety.trendmicro.com/

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

15-2



16-1

Chapter 16

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

16-2

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:

https://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



Appendix A

Ports used by the appliance

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

TABLE A-1. Port 22

Port	22
Protocol	ТСР
Function	Listening
Purpose	Deep Discovery Inspector uses this port to:
	Connect to the preconfiguration console
	 Send logs and data to the Threat Management Services Portal if Deep Discovery Inspector is registered over SSH

TABLE A-2. Port 25

Port	25
Protocol	ТСР
Function	Outbound
Purpose	Deep Discovery Inspector sends notifications and scheduled reports through SMTP.

TABLE A-3. Port 53

Port	53
Protocol	TCP/UDP
Function	Outbound
Purpose	Deep Discovery Inspector uses this port for DNS resolution.

TABLE A-4. Port 67

Port	67
Protocol	UDP
Function	Outbound
Purpose	Deep Discovery Inspector sends requests to the DHCP server if IP addresses are assigned dynamically.

TABLE A-5. Port 68

Port	68
Protocol	UDP
Function	Listening
Purpose	Deep Discovery Inspector receives responses from the DHCP server.

TABLE A-6. Port 80

Port	80
Protocol	ТСР
Function	Listening
Purpose	Deep Discovery Inspector connects to other computers and integrated TrendMicro products and hosted services through this port.Share threat intelligence information with other products
Function	Outbound

Purpose	Purpose	Deep Discovery Inspector connects to other computers and integrated Trend Micro products and hosted services through this port.
		Communicate with Trend Micro Apex Central if Deep Discovery Inspector is registered over HTTP
		 Update components by connecting to the ActiveUpdate server

TABLE A-7. Port 123

Port	123
Protocol	UDP
Function	Outbound
Purpose	Deep Discovery Inspector uses this port to connect to the NTP server to synchronize time.

TABLE A-8. Port 137

Port	137
Protocol	UDP
Function	Outbound
Purpose	Deep Discovery Inspector uses NetBIOS to resolve IP addresses to host names.

TABLE A-9. Port 161

Port	161
Protocol	UDP
Function	Listening
Purpose	Deep Discovery Inspector uses this port for SNMP agent listening and protocol translation.

TABLE A-10. Port 162

Port	162
Protocol	UDP
Function	Outbound

Purpose Deep Discovery Inspector uses this port to send SNMP trap notifications.
--

TABLE A-11. Port 389

Port	389
Protocol	TCP/UDP
Function	Outbound
Purpose	Deep Discovery Inspector uses this port to retrieve user information from LDAP servers.
	Note This is the default port. Configure this port through the management console.

TABLE A-12. Port 443

Port	443
Protocol	ТСР
Function	Listening
Purpose	Deep Discovery Inspector uses this port to:Access the management console with a computer through HTTPS
Function	Outbound

Purpose	Deep Discovery Inspector uses this port to:
	Communicate with Deep Discovery Director - On-premises version
	 Note This is the default port. Configure this port through the management console. Communicate with Trend Micro Apex Central
	Note This is the default port. Configure this port through the management console.
	Communicate with Trend Micro Service Gateway
	Communicate with Trend Vision One
	 Connect to MITRE ATT&CK[™] Tactics and Techniques website
	Connect to Trend Micro Threat Connect
	Query Mobile App Reputation Service through Smart Protection Server
	Query Predictive Machine Learning engine
	Query the Web Reputation Services blocking reason
	Register to the mitigation server
	 Scan APK files and send detection information to the Mobile App Reputation Service
	Send files to Deep Discovery Analyzer for sandbox analysis
	Note This is the default port. Configure this port through the management console.
	 Send logs and data to the Threat Management Services Portal if Deep Discovery Inspector is using SSL encryption

Share anonymous threat information with the Smart Protection Network

- Share threat intelligence information with Trend Micro TXOne OT Defense Console
- Verify the safety of files through the Certified Safe Software Service

TABLE A-13. Port 465

Port	465
Protocol	ТСР
Function	Outbound
Purpose	Deep Discovery Inspector sends notifications and scheduled reports through SMTP over TCP with SSL/TLS encryption.

TABLE A-14. Port 514

Port	514
Protocol	UDP
Function	Outbound
Purpose	Deep Discovery Inspector sends logs to a syslog server over UDP. Note The port must match the syslog server.
	Note This is the default port. Configure this port through the management console.

TABLE A-15. Port 587

Port	587
Protocol	ТСР
Function	Outbound
Purpose	Deep Discovery Inspector sends notifications and scheduled reports through SMTP over TCP with STARTTLS encryption.

TABLE A-16. Port 601

Port	601
Protocol	ТСР
Function	Outbound
Purpose	Deep Discovery Inspector uses this port to send logs to a syslog server. Note The port must match the syslog server.
	Note This is the default port. Configure this port through the management console.

TABLE A-17. Port 636

Port	636
Protocol	UDP
Function	Outbound
Purpose	Deep Discovery Inspector uses this port to retrieve user information from LDAP servers.
	Note This is the default port. Configure this port through the management console.

TABLE A-18. Port 3268

Port	3268
Protocol	ТСР
Function	Outbound

1	
Purpose	Deep Discovery Inspector uses this port to retrieve user information from LDAP
	servers.

TABLE A-19. Port 3269

Port	3269
Protocol	ТСР
Function	Outbound
Purpose	Deep Discovery Inspector uses this port to retrieve user information from LDAP servers.

TABLE A-20. Port 4343

Port	4343
Protocol	ТСР
Function	Outbound
Purpose	Communicate with Smart Protection Server

TABLE A-21. Port 5275

Port	5275
Protocol	ТСР
Function	Outbound
Purpose	 Query Web Reputation Services through Smart Protection Server using HTTPS
	Query Web Reputation Services through Service Gateway Smart Protection Server using HTTPS

TABLE A-22. Port 6514

Port	6514
Protocol	ТСР
Function	Outbound

Purpose Deep Discovery Inspector sends logs to a syslog server over TCP with SSL encryption. Image: Note The port must match the syslog server. Image: Note This is the default port. Configure this port through the management console.

TABLE A-23. Port 8514

Port	8514
Protocol	UDP
Function	Outbound
Purpose	Deep Discovery Inspector sends syslog information to Deep Discovery Advisor if Deep Discovery Inspector is integrated with Deep Discovery Advisor.
	Note This is the default port. It can be configured through the management console, and it must match the syslog settings on Deep Discovery Advisor.

TABLE A-24. Port 8080

Port	8080
Protocol	ТСР
Function	Listening

Purpose	Deep Discovery Inspector uses this port to share threat intelligence with other products.
	Note This is the default port. Configure this port through the management console.





Index

D

documentation feedback, 16-2

S

support resolve issues faster, 14-3





TREND MICRO INCORPORATED

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



Item Code: APEM69898/240430