Trend Micro™

Deep Discovery Inspector

6.6

Inline (LAN Bypass) Network Interface Card Installation 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:

http://docs.trendmicro.com

Trend Micro, the Trend Micro t-ball logo, Deep Discovery Inspector, Apex Central, and Trend Micro Control Manager 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 © 2023. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM69763/230720

Release Date: July 2023

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.

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

Chapter 1: Installation Planning

Items to Prepare 1-2

Chapter 2: Installation

Installing the Inline (LAN Bypass) Network Interface Card 2-2

Checking the Inline (LAN Bypass) Network Interface Card Status 2-6

Chapter 3: Frequently Asked Questions

What Happens If Deep Discovery Inspector Enters Inline Appliance Mode? 3-2

Which PCI-e Slot Should I Use to Install the Inline (LAN Bypass) Network Interface Card? 3-2

What Happens If the Inline (LAN Bypass) Network Interface Card Is Removed or If the Inline (LAN Bypass) Network Interface Card Stops Working While Deep Discovery Inspector Is in Inline Appliance Mode? 3-2

Index

Index IN-1

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:

TABLE 1. Product Documentation

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: https://success.trendmicro.com

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

Chapter 1

Installation Planning

Items to Prepare

- **Deep Discovery Inspector appliance running Deep Discovery Inspector 6.2**

  Supported models:

  - 520
  - 530
  - 1200
  - 1300
  - 4200
  - 9200

Important

Installing an inline (LAN Bypass) network interface card in Deep Discovery Inspector 530/1300 requires removing the appliance's COM port permanently. If you need the COM port for Deep Discovery Inspector's preconfiguration, Trend Micro recommends using Dell's iDRAC instead.

- **Inline (LAN bypass) network interface card**

  Select the appropriate card according to the network throughput. Supported cards:

  - Dual Port 1GbE Copper Bypass Card for TLS Inspection
  - Dual Port 10GbE Fiber-SR Bypass Card for TLS Inspection

Chapter 2

Installation

Installing the Inline (LAN Bypass) Network Interface Card

Procedure

1. Shutdown Deep Discovery Inspector.

   Go to **Administration** > **System Maintenance** > **Power Off / Restart** and power off the system.

2. Disconnect the power cord from the appliance.

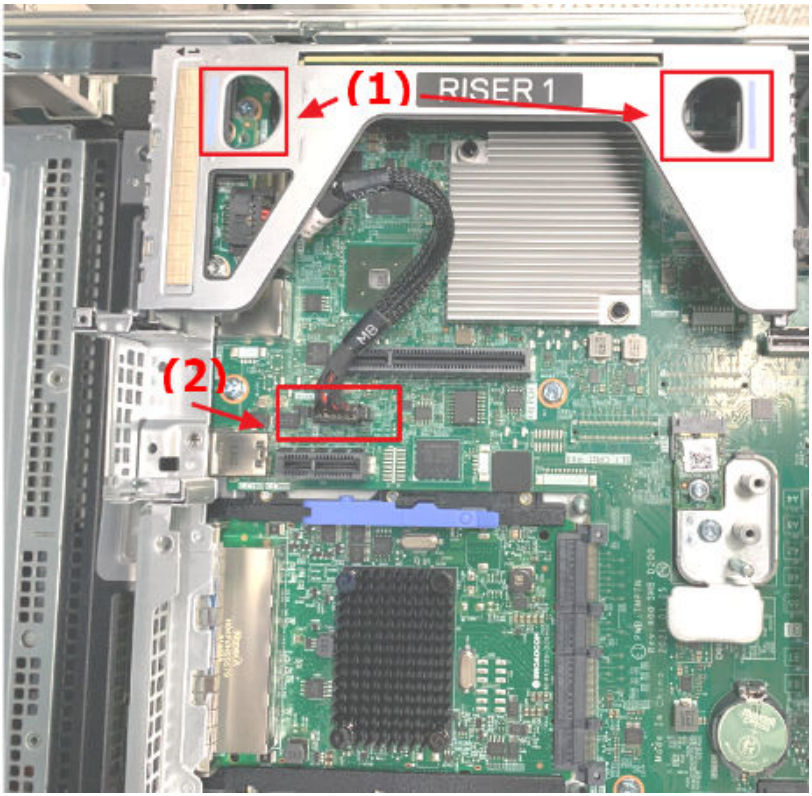
3. Install the Inline (LAN bypass) network interface card in the appliance

   a. Remove the server's top cover.

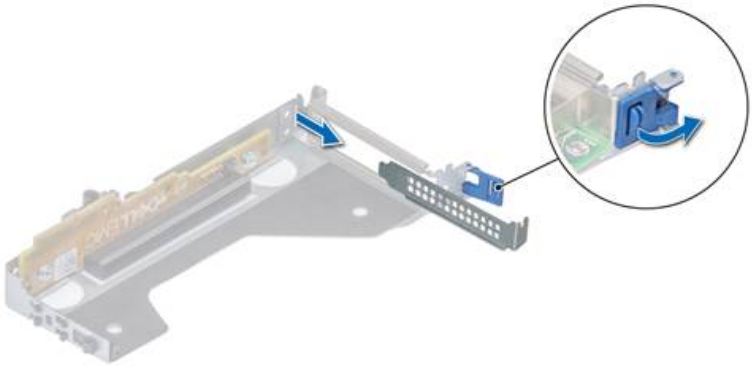
   b. (For Deep Discovery Inspector 530/1300 only) Remove the COM port from the appliance.

      1. Hold the card riser from the sides marked with blue (1), then lift the card riser.

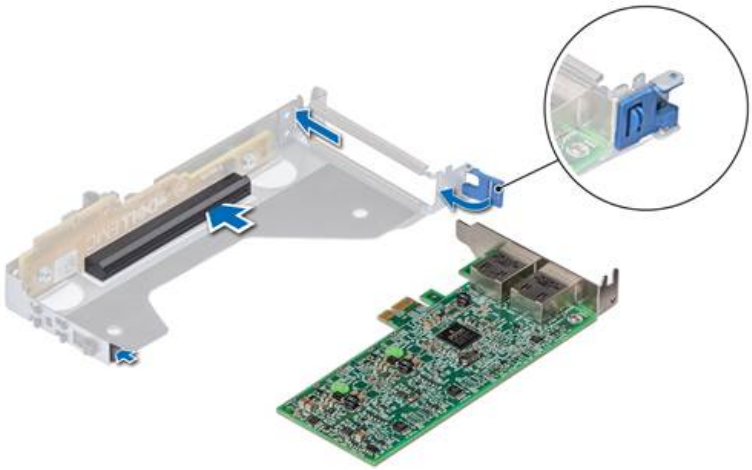
      2. Disconnect the COM port connector from the motherboard (2).



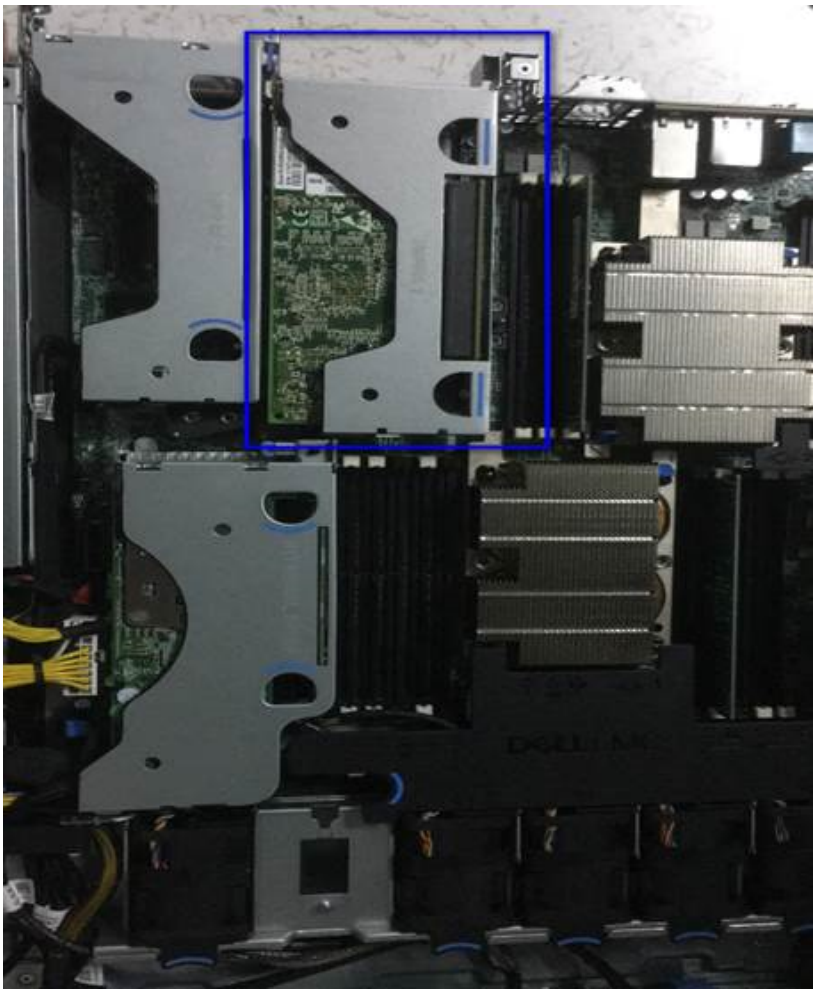
c. Open the card retention latch and remove the PCI slot cover of an empty PCI-e slot



d. Align the card with the server's PCI-e slot, push the card in firmly until the card is connected, then close the card retention latch.



e. Secure the card holder to the server chassis.



f. Close up the server.

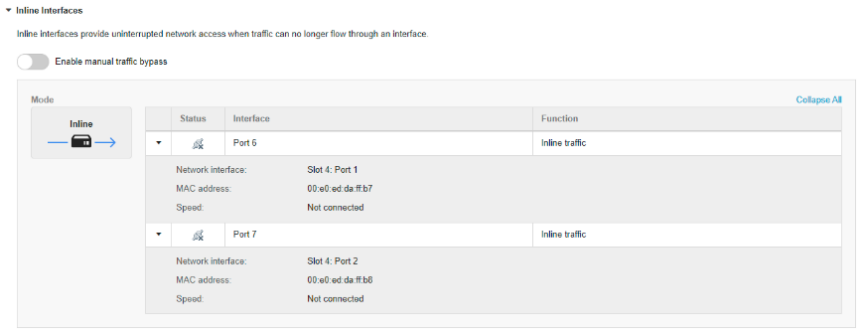
Checking the Inline (LAN Bypass) Network Interface Card Status

After installing, check the card status on the Deep Discovery Inspector management console.

Procedure

1. Power on the appliance.
2. In the management console, go to **Administration** > **System Settings** > **Network Interface**.
3. Check the card status.

   If the inline (LAN Bypass) network interface card is installed correctly, the **Inline Interfaces** section appears.



Chapter 3

Frequently Asked Questions

What Happens If Deep Discovery Inspector Enters Inline Appliance Mode?

Deep Discovery Inspector does not support inline and out-of-band deployment at the same time. If Deep Discovery Inspector was originally deployed in offline mode, enabling inline appliance mode stops network traffic monitoring from mirror ports, and only traffic flowing through inline ports is inspected.

Note

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

Which PCI-e Slot Should I Use to Install the Inline (LAN Bypass) Network Interface Card?

Trend Micro recommends using any empty PCI-e slot to install an inline (LAN Bypass) network interface card.

Important

Moving installed cards to different slots before installing an inline (LAN Bypass) network interface card results in unexpected configuration changes.

What Happens If the Inline (LAN Bypass) Network Interface Card Is Removed or If the Inline (LAN Bypass) Network Interface Card Stops Working While Deep Discovery Inspector Is in Inline Appliance Mode?

Deep Discovery Inspector automatically switches to offline mode, and stops inspecting TLS traffic. All the events associated to this change are recorded into the system logs.

Index

TREND MICRO

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: APEM69763/230720