Trend Micro™ Threat Discovery Appliance Quick Start Guide

Trend Micro™ Threat Discovery Appliance is a next-generation network monitoring device that uses a combination of intelligent rules, algorithms, and signatures to detect a variety of malware including worms, Trojans, backdoor programs, viruses, spyware/grayware, adware, and other threats. The detection is done at layers 2 to 7 of the Open Systems Interconnection Reference Model (OSI model).

The appliance delivers high-performance throughput and availability and provides critical security information, alerts, and reports to IT administrators. Trend Micro Control Manager™ can manage Threat Discovery Appliance.

The Threat Discovery Appliance documentation consists of the following:

- Quick Start Guide — User-friendly instructions on connecting Threat Discovery Appliance to your network and on performing initial configuration
- Administrator's Guide — Instructions for configuring and managing the appliance
- Help — Helps you configure all features through the user interface. To access the Help, open the product console and then click the help icon
- Readme — Late-breaking news, known issues, installation tips, and other important information
- License Agreement — License agreements for Threat Discovery Appliance and third-party applications

1 Opening and Inspecting the Carton

Verify that the Threat Discovery Appliance carton contains the following items:

Threat Discovery Appliance

Rack Rail Box

Documentation

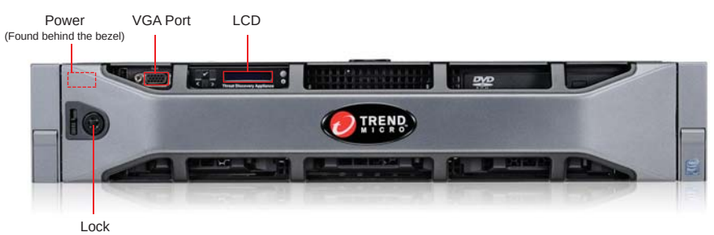
Serial Cable (RS-232)

Power Cords

2 Examining Threat Discovery Appliance

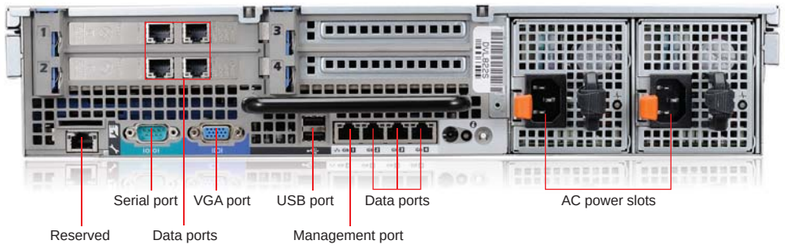
Familiarize yourself with the front and back panels of the appliance.

Threat Discovery Appliance front panel



Light	State	Description
Power	Steady	Power on
	Off	Power off

Threat Discovery Appliance back panel



Note: The two power slots are for protection in case one of the power slots fails.

Port	Cable	Speed	Description
Data	Ethernet	10/100/1000 Mbps	A total of 7 data ports connected to the network
Management	Ethernet	10/100/1000 Mbps	A network port with a fixed IP address. You can upload operating system image files through this port in rescue mode.
Serial	Serial		Serial connection to access the preconfiguration console
VGA	VGA		VGA connection to access the preconfiguration console
USB		2.0	Reserved

3 Understanding Operating Modes and Network Topology

Threat Discovery Appliance is deployed offline. This means that Threat Discovery Appliance does not interrupt network traffic. A switch monitors both internal and external traffic, and passes the information to Threat Discovery Appliance. Threat Discovery Appliance then uses this information to monitor known and potential threats.

You can connect switches with a mirror port to any of the 7 data ports. The appliance uses these ports as listening ports and will not interrupt traffic handled by the switches.

4 Mounting Threat Discovery Appliance

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

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

5 Performing Initial Configuration

Perform initial configuration from the preconfiguration console. There are various ways to access the console:

- **From a monitor with a VGA port**:
  Connect the VGA port to the VGA port of Thread Discovery Appliance using a VGA cable.
- **From a computer with an ethernet port**:
  A. Connect the ethernet port to the management port of Thread Discovery Appliance using a general ethernet cable.
  B. Use an SSH communication application such as PuTTY.
  C. Use the following values:
  - IP address (for SSH connection only): by default, it is 192.168.252.1
  - User name: tda
  - Password: [press Enter]
  - Port number: 22
- **From a computer with a serial port:**
  A. Connect the serial port to the serial port of Threat Discovery Appliance using an RS-232 serial cable.
  B. Access the console using a serial communication application such as HyperTerminal.
  C. Use the following values:
  - Bits per second: 115200
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None

To perform initial configuration:

1. When the preconfiguration screen opens, type the default password **admin**.
2. Press **Enter** twice. The Main Menu appears.
3. Scroll down to **2) Device Settings**. Press **Enter**. The device settings screen appears.
4. Configure the following network settings:
   - **IP address** – by default, this is 192.168.252.1
   - **Netmask** – by default, this is 255.255.255.0
   - **Default Gateway** - by default, this is 192.168.252.254
   - **DNS server 1**
   - **DNS server 2**
   - **Host name** - by default, this is localhost
5. If you want to register the appliance to the Control Manager server, select yes. You can also register Threat Discovery Appliance to Control Manager from the product console.
6. Return to the Main Menu and scroll down to **7) Log Off with saving**. Press **Enter**.

6 Connecting Threat Discovery Appliance to your Network

Threat Discovery Appliance begins monitoring traffic after the boot up procedure is complete and when it is connected to your network.

To connect the appliance to your network:

1. Plug in both of the included power cables into the device power receptacle and then plug the cables into a power source.
2. Turn on the power switch.
3. Connect one end of an Ethernet cable to any of the 7 data ports and the other to the device from which Threat Discovery Appliance will receive traffic, such as a core switch.

7 Accessing the Product Console

To access the product console:

1. From a computer on your network that can access Threat Discovery Appliance, open Internet Explorer (version 6 or 7).

   Note: Set up the computer with the same Subnet as the device management IP address. By default, the product console URL is https://192.168.252.1.

2. Type the default password **admin** and click **Log On**.

   *Note: Configure the Network Configuration settings for more accurate detection. Please refer to the Help or **Administrator's Guide** for more information.*

8 Contact Information

- Web site: http://www.trendmicro.com
- Phone: +1 (800) 228-5651 or +1 (408) 257-1500
- Address: Trend Micro Inc., 10101 N. De Anza Blvd., Cupertino CA – 95014, USA

Item Code: APEQ24214/90811