Trend Micro™ Threat Discovery Appliance Quick Start Guide

The Trend Micro™ Threat Discovery Appliance device 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. This 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 the Threat Discovery Appliance device.

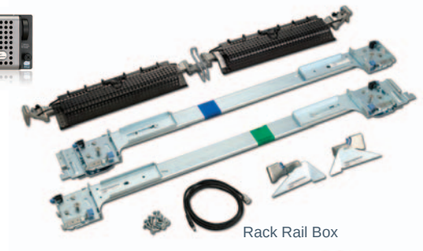
The Threat Discovery Appliance documentation consists of the following:

- 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
- Online help — Helps you configure all features through the user interface. To access the online help, open the Web 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

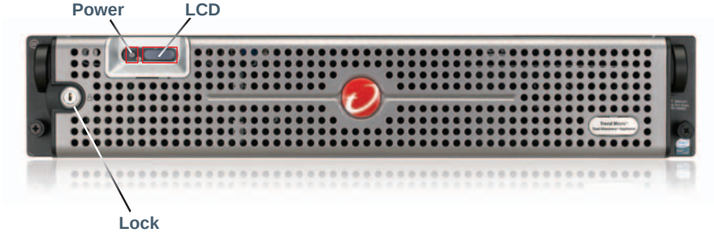
Serial Cable (RS-232)

Power Cords

2 Examine the Threat Discovery Appliance Device

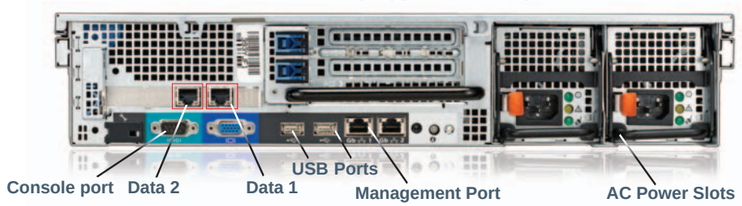
Familiarize yourself with the device's front and back panels.

Threat Discovery Appliance front panel



Light	State	Description
PWR	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 1	Ethernet	10/100/1000 Mbps	Data port that connects to the network.
Data 2	Ethernet	10/100/1000 Mbps	Data port that connects to the network.
MANAGED	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. The Managed port is also known as Management port.
CONSOLE	Serial		Serial connection to access the command line interface menu for initial setup and troubleshooting.
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 the network. The switch monitors both internal and external traffic, and passes the information to the device. Threat Discovery Appliance then uses this information to monitor known and potential threats.

You can connect to either Data 1 or Data 2. The device uses these as listening ports and will not interrupt the current network segment. You can use Threat Discovery Appliance in segment switches and deploy the device anywhere a mirror port function for all monitored traffic is supported.

4 Mounting the Threat Discovery Appliance Device

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

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

5 Connecting a Computer to Threat Discovery Appliance

To perform initial configuration, connect a computer to Threat Discovery Appliance using one of the following ports:

- Using an application that supports SSH communication, connect an Ethernet cable to the Managed port. This port is compatible with 10/100/1000 Mbps networks.
- Using an application that supports serial communication, such as HyperTerminal, connect a RS232 serial cable to the Console port.

6 Performing Initial Configuration

To set up Threat Discovery Appliance, you must perform initial configuration steps through the Preconfiguration Console. You can access the Preconfiguration Console from the management port using the SSH application or from the serial console using HyperTerminal.

To perform initial configuration:

1. On the computer that you connected to the device in the previous step, open one of the following:
   - An SSH communication application if you connect to the Managed port.
   - A serial communication application if you connect to the Console port.
2. For an SSH connection, 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
3. For a serial connection, use the following values:
   - **Bits per second:** 115200
   - **Data bits:** 8
   - **Parity:** None
   - **Stop bits:** 1
   - **Flow control:** None
4. After setting up the connections, access the Preconfiguration Console from the console port. The default password is admin.
5. Press **Enter** twice. The Main Menu appears.
6. Scroll down to **2) Device Settings**. Press **Enter**. The device settings screen appears.
7. 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
8. If you want to register the device to the Control Manager server, select yes. Alternatively, you can also register Threat Discovery Appliance to Control Manager using the web console.
9. Return to the Main Menu and scroll down to **7) Log Off with saving**. Press **Enter**.

7 Connecting Threat Discovery Appliance to your Network

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

To connect the device 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 the Data port 1 or 2 of the device and the other to the device from which Threat Discovery Appliance will receive traffic, such as a switch or router.

8 Accessing the Web Console

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

To access the Web 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.
2. By default, the Managed port IP address is https://192.168.252.1.
3. Type the default password admin and click **Log On**.

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

9 Contact Information

- Local offices: http://www.trendmicro.com/en/about/contact/us.htm
- Phone: +1 (800) 228-5651 or +1 (408) 257-1500
- Address: Trend Micro, 10101 N. De Anza Blvd., Cupertino CA – 95014, USA

Item Code: APEC23580/80307