TREND MICRO™
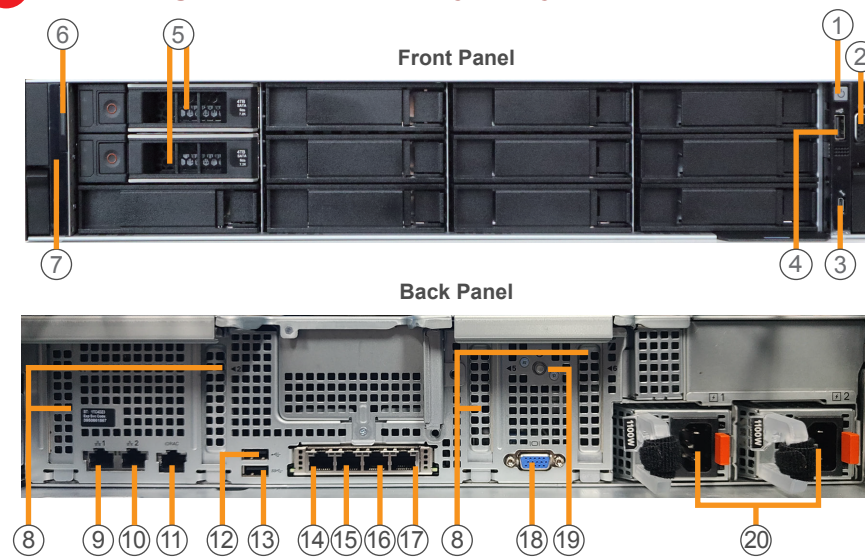# Deep Discovery™ Analyzer 1300 Quick Start Card

Deep Discovery Analyzer is a custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products. Deep Discovery Analyzer supports out-of-the-box integration with Trend Micro email and web security products, and can also be used to augment or centralize the sandbox analysis of other Deep Discovery products.

## 1 Opening and Inspecting the Carton

Verify that the Deep Discovery Analyzer carton contains the following items:

Rack rails

Document

Deep Discovery Analyzer appliance

Power Cords

## 2 Examining the Deep Discovery Analyzer Appliance

**Front Panel**

**Back Panel**

(1) Power-on indicator/button
(2) Front video connector
(3) iDRAC Direct port
(4) USB 2.0 connector
(5) Hard drives
(6) System health and system ID indicator
(7) Status LED indicators
(8) Expansion card slots*
(9) Default management port eth0
(10) eth1
(11) iDRAC port
(12) USB 2.0 connector
(13) USB 3.0 connector
(14) eth2
(15) eth3
(16) eth4
(17) eth5
(18) Back video connector
(19) System identification button
(20) Power supply connectors

*Expansion card slots: For optional fiber Ethernet NIC installation. The system supports up to two additional Ethernet ports.
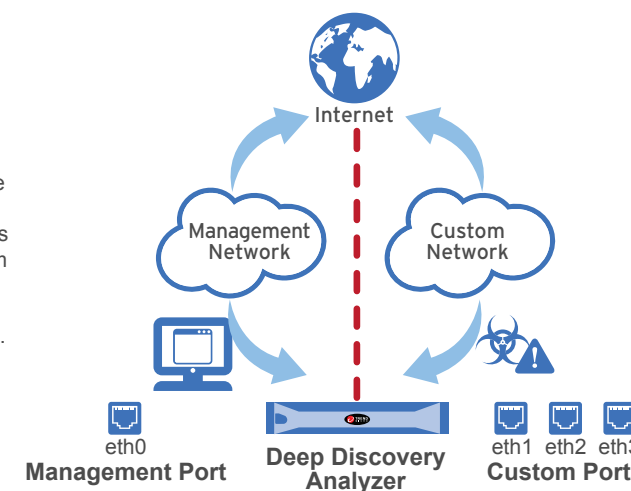
• **Management port**: Connects the appliance to the management network. You can configure an interface (default is eth0) or a NIC teaming port as the management port.
• **Custom port**: Connects the appliance to custom networks that are reserved for sandbox analysis. You can configure an interface or a NIC teaming port as a custom port.
• **High availability on eth3**: Connects the appliance to eth3 of an identical appliance.

## 3 Recommended Network Environment

Deep Discovery Analyzer requires connection to a management network, which usually is the organization's intranet. After deployment, administrators can perform configuration tasks from any computer on the management network.

Trend Micro recommends using a custom network for sample analysis. Custom networks ideally are connected to the Internet but may be configured with their own network settings. Deep Discovery Analyzer provides the option to configure proxies for custom networks, as well as providing support for proxy authentication.

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

Internet

Management Network

Custom Network

eth0
**Management Port**

**Deep Discovery Analyzer**

eth1 eth2 eth3
**Custom Ports**

## 4 Deployment Checklist

| Requirement | Details |
|---|---|
| Activation Code | Obtain from Trend Micro |
| Monitor and VGA cable | Connects to the VGA port of the appliance |
| USB keyboard | Connects to the USB port of the appliance |
| USB mouse | Connects to the USB port of the appliance |
| Ethernet cables | • One cable connects the management port of the appliance to the management network.<br>• One cable connects a custom port to an isolated network that is reserved for sandbox analysis.<br>• If using high availability, one cable connects eth3 to eth3 on an identical Deep Discovery Analyzer appliance. |
| Internet-enabled computer | A computer with the following software installed:<br>• Microsoft™ Edge™, Mozilla™ Firefox™, or Google™ Chrome™. |
| IP addresses | • One static IPv4 address in the management network.<br>• If sandbox instances require Internet connectivity, one extra IPv4 address for Virtual Analyzer.<br>• If using high availability, one extra virtual IP address. |

## 5 Setting Up the Hardware

1. 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.*

2. Connect the appliance to a power source.
3. Connect the monitor to the VGA port at the back of the appliance.

4. Connect the keyboard and mouse to the USB ports at the back of the appliance.
5. Connect the Ethernet cables to the management and custom ports.
6. Power on the appliance.

## 6 Performing Initial Configuration

1. On the preconfiguration console logon screen, type the following default logon credentials:
   • User name: **admin**
   • Password: **Admin1234!**

   *Note: The typed password characters do not appear on the screen.*

2. Select **Configure appliance IP address** and press **Enter**.
3. Specify the following network addresses.
   • IPv4 address: Must not conflict with the Virtual Analyzer addresses and custom network address
   • Subnet mask
   • IPv4 gateway: Must be in the same subnet as the IP address
   • IPv4 DNS server 1
4. Press **Tab** to navigate to **Save**, and then press **Enter**.

For additional configuration procedures, see the Getting Started chapter in the Administrator's Guide. Download the document at:

http://docs.trendmicro.com/en-us/enterprise/deep-discovery-analyzer.aspx

## 7 Accessing the Management Console

1. Using a supported web browser, open the management console at:
   https://<Deep Discovery Analyzer IP Address>/pages/login.php

   *Note:*
   • *Set the Internet Security level to Medium and enable ActiveX Binary and Script Behaviors.*
   • *Use the IP address that you specified during the initial configuration.*

2. On the logon screen, type the following default credentials:
   • User name: **admin**
   • Password: **Admin1234!**
3. Click **Log On**.
4. Change the default password.

## 8 Contact Information

• **Website:**
  http://www.trendmicro.com

• **List of worldwide offices and phone numbers:**
  http://www.trendmicro.com/us/about-us/contact/index.html

Item Code: APEQ759852/230927