

5.1 Deep Discovery Analyzer

Installation and Upgrade Guide

Breakthrough Protection Against APTs and Targeted Attacks



Endpoint Security



Network Security



Protected Cloud



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>

© 2015 Trend Micro Incorporated. All Rights Reserved. Trend Micro, the Trend Micro t-ball logo, and 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.

Document Part No.: APEM56867/150213

Release Date: April 2015

Protected by U.S. Patent No.: Patents pending.

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 in the Trend Micro Online Help and/or the Trend Micro Knowledge Base at the Trend Micro website.

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 docs@trendmicro.com.

Evaluate this documentation on the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Table of Contents

Preface

Preface	iii
Documentation	iv
Audience	v
Document Conventions	v
Terminology	vi
About Trend Micro	vii

Chapter 1: Preparing to Deploy Deep Discovery Analyzer

Deployment Overview	1-2
Product Specifications	1-2
Recommended Network Environment	1-2
Cluster Deployment	1-3
Network Settings	1-5
Deployment Requirements and Checklists	1-5
Items to Obtain from Trend Micro	1-5
Items to Prepare	1-6
Logon Credentials	1-7
Ports Used by Deep Discovery Analyzer	1-7

Chapter 2: Installing Deep Discovery Analyzer

Installation Tasks	2-2
Setting Up the Hardware	2-2
Installing Deep Discovery Analyzer	2-3

Chapter 3: Using the Preconfiguration Console

The Preconfiguration Console	3-2
Preconfiguration Console Basic Operations	3-3
Configuring Network Addresses on the Preconfiguration Console	3-4

Chapter 4: Migrating Deep Discovery Analyzer 5.0 to 5.1

Migration Tasks	4-3
Preparing a Windows 7 Samba Server	4-4
Exporting Configuration Settings and Data	4-5
Importing Configuration Settings and Data	4-6
Clearing the Browser Cache	4-7
Restoring Services After Migration	4-8

Chapter 5: Technical Support

Troubleshooting Resources	5-2
Trend Community	5-2
Using the Support Portal	5-2
Security Intelligence Community	5-3
Threat Encyclopedia	5-3
Contacting Trend Micro	5-3
Speeding Up the Support Call	5-4
Sending Suspicious Content to Trend Micro	5-5
File Reputation Services	5-5
Email Reputation Services	5-5
Web Reputation Services	5-5
Other Resources	5-6
TrendEdge	5-6
Download Center	5-6
TrendLabs	5-6

Index

Index	IN-1
-------------	------

Preface

Preface

Welcome to the Deep Discovery Analyzer *Installation and Upgrade Guide*. This guide contains information about the requirements and procedures for deploying, installing and migrating Deep Discovery Analyzer.

Documentation

The documentation set for Deep Discovery Analyzer includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	<p>PDF documentation provided with the product or downloadable from the Trend Micro website.</p> <p>The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Analyzer, and explanations on Deep Discovery Analyzer concepts and features.</p>
Installation and Upgrade Guide	<p>PDF documentation provided with the product or downloadable from the Trend Micro website.</p> <p>The Installation and Upgrade Guide discusses requirements and procedures for installing and upgrading Deep Discovery Analyzer.</p>
Quick Start Guide	<p>The Quick Start Guide provides user-friendly instructions on connecting Deep Discovery Analyzer to your network and on performing the initial configuration.</p>
Readme	<p>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.</p>
Online Help	<p>Web-based documentation that is accessible from the Deep Discovery Analyzer management console.</p> <p>The Online Help contains explanations of Deep Discovery Analyzer components and features, as well as procedures needed to configure Deep Discovery Analyzer.</p>
Support Portal	<p>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:</p> <p>http://esupport.trendmicro.com</p>

View and download product documentation from the Trend Micro Documentation Center:

<http://docs.trendmicro.com/en-us/home.aspx>

Audience

The Deep Discovery Analyzer 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
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output

CONVENTION	DESCRIPTION
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

Terminology

TERMINOLOGY	DESCRIPTION
ActiveUpdate	A component update source managed by Trend Micro. ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, program, and other Trend Micro component files through the Internet.
Administrator	The person managing Deep Discovery Analyzer
Custom port	A hardware port that connects Deep Discovery Analyzer to an isolated network dedicated to sandbox analysis
Dashboard	UI screen on which widgets are displayed
Management console	A web-based user interface for managing a product.

TERMINOLOGY	DESCRIPTION
Management port	A hardware port that connects to the management network.
Sandbox image	A ready-to- use software package (operating system with applications) that require no configuration or installation. Virtual Analyzer supports only image files in the Open Virtual Appliance (OVA) format.
Sandbox instance	A single virtual machine based on a sandbox image.
Threat Connect	A Trend Micro service that correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network. By providing on-demand access to Trend Micro intelligence databases, Threat Connect enables you to identify and investigate potential threats to your environment.
Virtual Analyzer	A secure virtual environment used to manage and analyze samples submitted by Trend Micro products. Sandbox images allow observation of file and network behavior in a natural setting.
Widget	A customizable screen to view targeted, selected data sets.

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

<http://www.trendmicro.com>

Trend Micro and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

Chapter 1

Preparing to Deploy Deep Discovery Analyzer

This chapter discusses the items you need to prepare to deploy Deep Discovery Analyzer and connect it to your network.

If Deep Discovery Analyzer is already deployed on your network and you have a patch, service pack, or hot fix to apply to it, see the *Deep Discovery Analyzer Administrator's Guide*.

Deployment Overview

Product Specifications

The standard Deep Discovery Analyzer appliance has the following specifications.

FEATURE	SPECIFICATIONS
Rack size	2U 19-inch standard rack
Availability	Raid 5 configuration
Storage size	2 TB free storage
Connectivity	<ul style="list-style-type: none">• Management port: 1 x 10Base-T/100Base-TX/1000Base-T• Custom ports: 3 x 10Base-T/100Base-TX/1000Base-T
Dimensions (WxDxH)	48.2 cm (18.98 in) x 75.58 cm (29.75 in) x 8.73 cm (3.44 in)
Maximum weight	32.5 kg (71.65 lb)
Operating temperature	10 °C to 35 °C at 10% to 80% relative humidity (RH)
Power	750W , 120-240 VAC 50/60 Hz

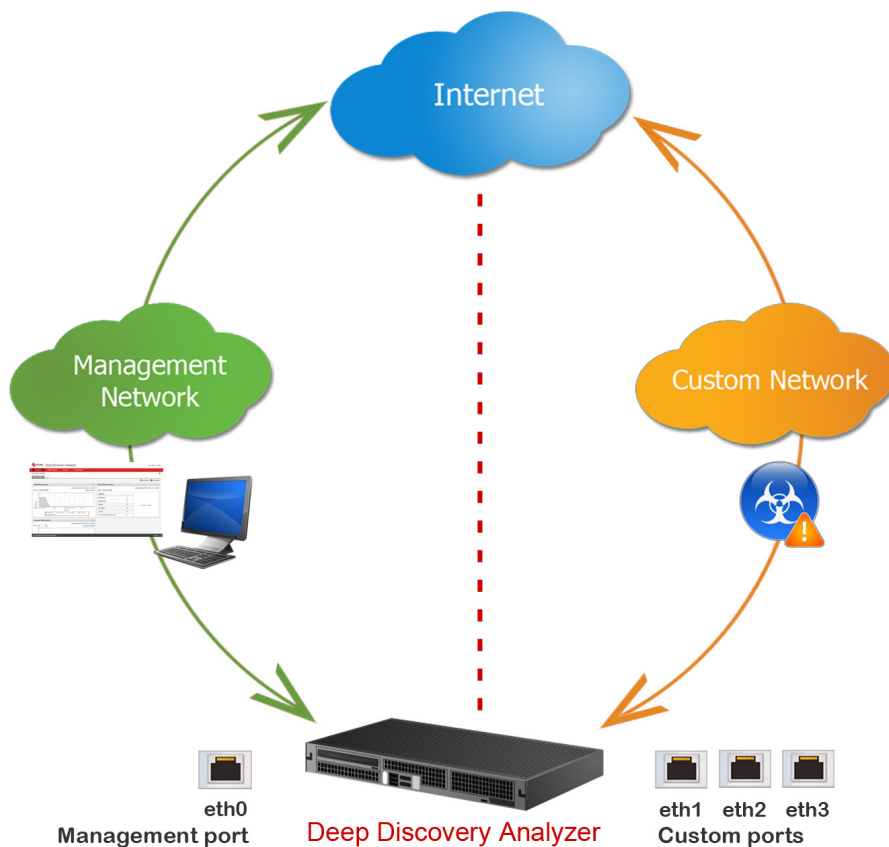
Contact Trend Micro if the appliance you are using does not meet these hardware specifications.

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 do not have proxy settings, proxy authentication, and connection restrictions.

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



Cluster Deployment

In a cluster environment, one appliance acts as the primary appliance and the rest as secondary appliances.

In this environment:

- The appliance in primary mode retains all configuration settings.
- The appliances in secondary mode identify the primary appliance using its IP address.
- The secondary appliances are automatically configured based on the settings of the primary appliance.

Cluster Deployment Tasks

Procedure

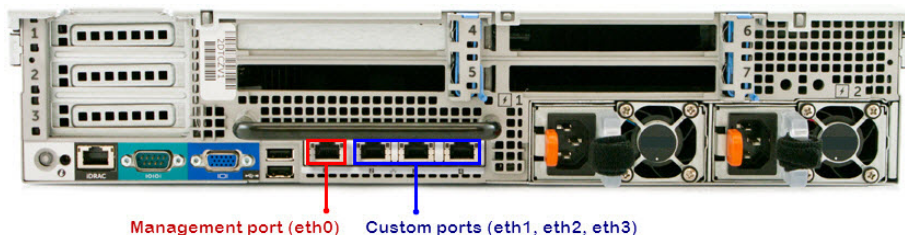
1. Perform the installation and deployment tasks.
 - a. Review the deployment requirements and checklists.

For details, see [Deployment Requirements and Checklists on page 1-5](#).
 - b. Perform the installation tasks.

For details, see [Installation Tasks on page 2-2](#).
 2. On the management console, go to **Administration > System Maintenance** and click the **Cluster** tab.
 3. Select the **Cluster Mode**.
 - **Primary mode**
 - **Secondary mode**
 4. Type the **Primary appliance IP address** and **Primary appliance API key** if **Secondary mode** was selected.
 5. Click **Save**.
-

Network Settings

Ports are found at the back of the appliance, as shown in the following image.



Network interface ports include:

- **Management port (eth0):** Connects the appliance to the management network
- **Custom ports (eth1, eth2, eth3):** Connect the appliance to isolated networks that are reserved for sandbox analysis

Deep Discovery Analyzer requires one available static IP address in the management network.

If sandbox instances require Internet connectivity during sample analysis, Trend Micro recommends allocating one extra IP address for Virtual Analyzer. The **Sandbox Management > Network Connection** screen allows you to specify static or DHCP addresses. For more information, see the *Deep Discovery Analyzer Administrator's Guide*.

Deployment Requirements and Checklists

Items to Obtain from Trend Micro

1. Deep Discovery Analyzer appliance
2. Deep Discovery Analyzer installation CD

3. Activation Code

Items to Prepare

REQUIREMENT	DETAILS
Monitor and VGA cable	Connects to the VGA port of the appliance
USB keyboard	Connects to a USB port of the appliance
USB mouse	Connects to a USB port of the appliance
Ethernet cables	<ul style="list-style-type: none">• One cable connects the management port of the appliance to the management network.• One cable connects a custom port to an isolated network that is reserved for sandbox analysis.
Internet-enabled computer	A computer with the following software installed: <ul style="list-style-type: none">• Microsoft Internet Explorer® 9 or 10, Google Chrome™, or Mozilla Firefox®• Adobe® Flash® 10 or later
IP addresses	<ul style="list-style-type: none">• One static IP address in the management network• If sandbox instances require Internet connectivity, one extra IP address for Virtual Analyzer
Third party software licenses	Licenses for all third party software installed on sandbox images

Logon Credentials

CONSOLE	PURPOSE	DEFAULT CREDENTIALS	YOUR INFORMATION
Preconfiguration console	Perform initial configuration tasks. See Configuring Network Addresses on the Preconfiguration Console on page 3-4 .	<ul style="list-style-type: none"> Deep Discovery Analyzer login (not configurable) : <code>admin</code> Password: <code>admin</code> 	Password:
Management console	<ul style="list-style-type: none"> Configure product settings View and download reports 	<ul style="list-style-type: none"> User name (not configurable) : <code>admin</code> Password: <code>Admin1234!</code> 	Password:
		Other user accounts (configured on the management console, in Administration > Account Management)	User account 1: User name: Password:
			User account 2: User name: Password:

Ports Used by Deep Discovery Analyzer

The following table shows the ports that are used with Deep Discovery Analyzer and why they are used.

PORT	PROTOCOL	FUNCTION	PURPOSE
21	TCP	Outbound	Deep Discovery Analyzer uses the specified port to send backup data to FTP servers.
22	TCP	Inbound and outbound	Deep Discovery Analyzer uses this port to: <ul style="list-style-type: none">• Access the preconfiguration console with a computer through SSH• Send backup data to an SFTP server
25	TCP	Outbound	Deep Discovery Analyzer sends reports through SMTP.
53	TCP/UDP	Outbound	Deep Discovery Analyzer uses this port for DNS resolution.
67	UDP	Outbound	Deep Discovery Analyzer sends requests to the DHCP server if IP addresses are assigned dynamically.
68	UDP	Inbound	Deep Discovery Analyzer receives responses from the DHCP server.
80	TCP	Inbound and outbound	Deep Discovery Analyzer connects to other computers and integrated Trend Micro products and hosted services through this port. In particular, it uses this port to: <ul style="list-style-type: none">• Connect to Customer Licensing Portal to manage the product license• Connect to Community File Reputation services when analyzing file samples• Connect to Web Reputation Services when analyzing URL samples

PORT	PROTOCOL	FUNCTION	PURPOSE
123	UDP	Outbound	Deep Discovery Analyzer uses this port to synchronize system time with that of time servers.
137	UDP	Outbound	Deep Discovery Analyzer uses this port for NetBIOS name queries.
443	TCP	Inbound and outbound	<p>Deep Discovery Analyzer uses this port to:</p> <ul style="list-style-type: none"> • Access the management console with a computer through HTTPS • Communicate with other Deep Discovery Analyzer appliances in a cluster environment • Communicate with Trend Micro Control Manager • Connect to Trend Micro Threat Connect • Connect to Web Reputation Services to query the blocking reason • Receive files from a computer with Manual Submission Tool • Receive samples from integrated products • Send anonymous threat information from Smart Feedback • Send Suspicious Objects list and analysis information to integrated products • Update components by connecting to the ActiveUpdate server • Verify the safety of files through Certified Safe Software Service

PORT	PROTOCOL	FUNCTION	PURPOSE
514	UDP	Outbound	Deep Discovery Analyzer uses this port as the recommended port to send logs to syslog servers through UDP.
601	TCP	Outbound	Deep Discovery Analyzer uses this port as the recommended port to send logs to syslog servers through TCP.
5274	TCP	Outbound	Deep Discovery Analyzer uses this port as the default port to connect to the Smart Protection Server for web reputation services.
User-defined		Outbound	Deep Discovery Analyzer uses the specified port to send logs to syslog servers.

Chapter 2

Installing Deep Discovery Analyzer

This chapter discusses the Deep Discovery Analyzer installation tasks.

Deep Discovery Analyzer is already installed on new appliances. Perform the tasks only if you need to reinstall or upgrade the firmware.

Installation Tasks

Procedure

1. Prepare the appliance for installation. For details, see [Setting Up the Hardware on page 2-2](#).
 2. Install Deep Discovery Analyzer. For details, see [Installing Deep Discovery Analyzer on page 2-3](#).
 3. Configure the IP address of the appliance on the preconfiguration console. For details, see [Configuring Network Addresses on the Preconfiguration Console on page 3-4](#).
-

Setting Up the Hardware

Procedure

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.

Deep Discovery Analyzer includes two 750-watt hot-plug power supply units. One acts as the main power supply and the other as a backup. The corresponding AC power slots are located at the back of the appliance, as shown in the following image.



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.
 - **Management port:** A hardware port that connects Deep Discovery Analyzer to the management network
 - **Custom port:** A hardware port that connects Deep Discovery Analyzer to an isolated network dedicated to sandbox analysis
6. Power on the appliance.

**Note**

The power button is found on the front panel of the appliance, behind the bezel.

What to do next

Configure the IP address of the appliance on the preconfiguration console to complete the deployment process. For details, see [Configuring Network Addresses on the Preconfiguration Console on page 3-4](#).

Installing Deep Discovery Analyzer

Procedure

1. Power on the appliance.

**Note**

The power button is found on the front panel of the appliance, behind the bezel.

The **power-on self-test (POST)** screen appears.

```

F2 = System Setup
Lifecycle Controller Disabled
F11 = BIOS Boot Manager
F12 = PXE Boot
Two 2.00 GHz Six-core Processors, Bus Speed:7.20 GT/s, L2/L3 Cache:1.5 MB/15 MB
System running at 2.00 GHz
System Memory Size: 48.0 GB, System Memory Speed: 1333 MHz, Voltage: 1.35V

Dell Serial ATA AHCI BIOS Version 1.0.2
Copyright (c) 1988-2012 Dell Inc.
Port E: PLDS DVD-ROM DS-8D3SH

Initializing Intel(R) Boot Agent GE v1.3.76
PXE 2.1 Build 090 (WFM 2.0)
Press Ctrl+S to enter the Setup Menu._

```

2. Insert the CD containing the Deep Discovery Analyzer installation package.
3. Restart the appliance.

The **POST** screen appears.

```

F2 = System Setup
Lifecycle Controller Disabled
F11 = BIOS Boot Manager
F12 = PXE Boot
Two 2.00 GHz Six-core Processors, Bus Speed:7.20 GT/s, L2/L3 Cache:1.5 MB/15 MB
System running at 2.00 GHz
System Memory Size: 48.0 GB, System Memory Speed: 1333 MHz, Voltage: 1.35V

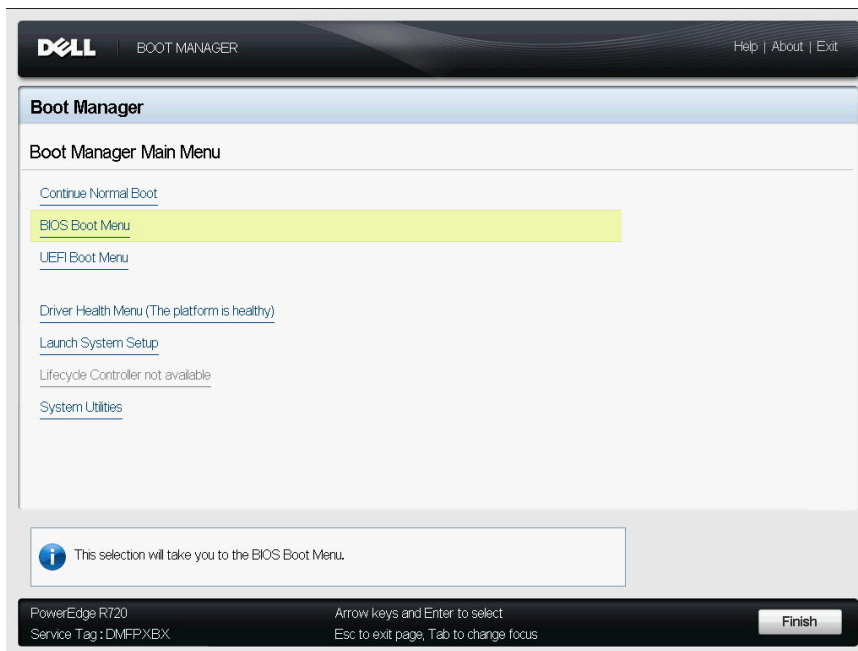
Dell Serial ATA AHCI BIOS Version 1.0.2
Copyright (c) 1988-2012 Dell Inc.
Port E: PLDS DVD-ROM DS-8D3SH

Initializing Intel(R) Boot Agent GE v1.3.76
PXE 2.1 Build 090 (WFM 2.0)
Press Ctrl+S to enter the Setup Menu._

```

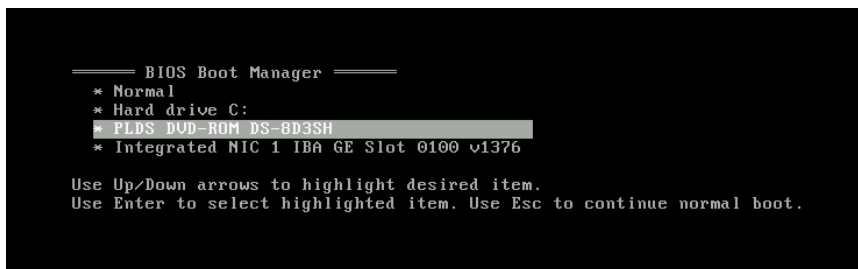
4. Press F11.

The **Boot Manager** screen appears.



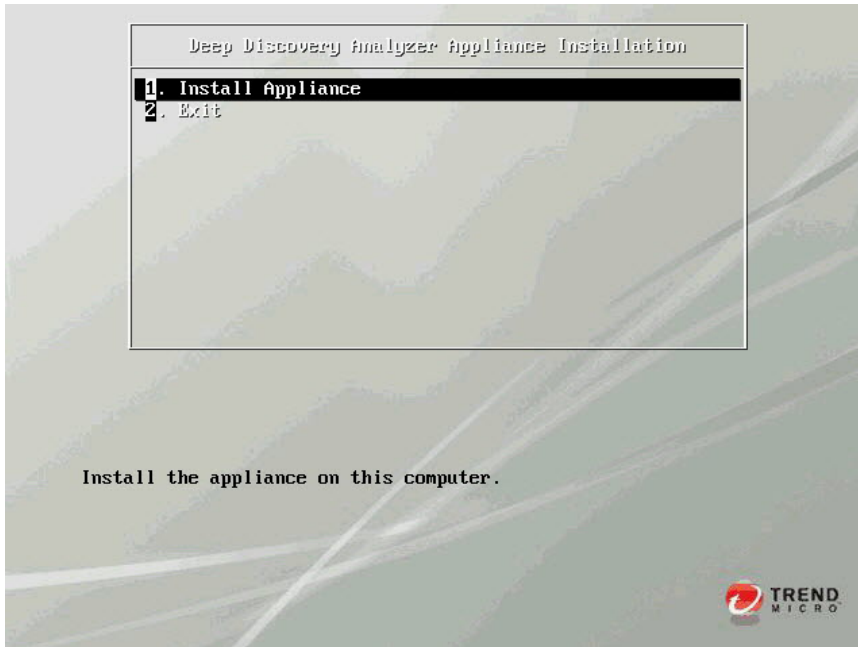
5. Under **Boot Manager Main Menu**, select **BIOS Boot Menu** and press **Enter**.

The **BIOS Boot Manager** screen appears.



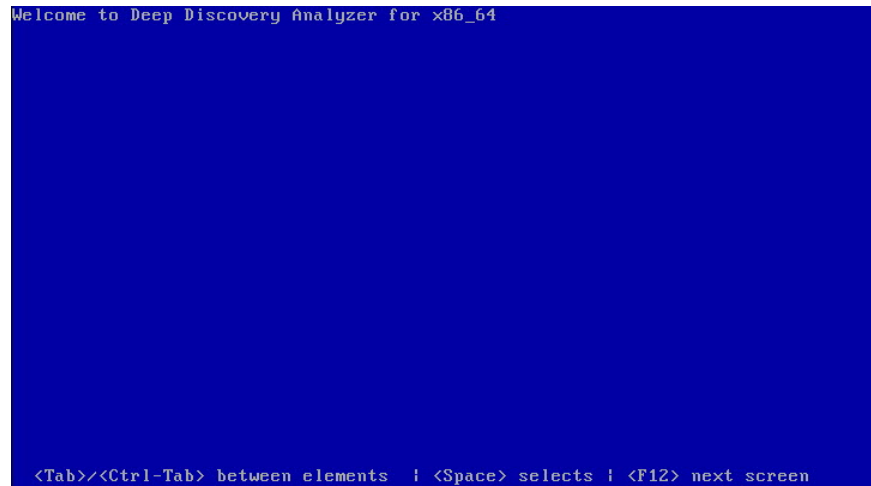
6. Select **PLDS DVD-ROM DS-8D3SH** and press **Enter**.

The **Deep Discovery Analyzer Appliance Installation** screen appears.



7. Select **1. Install Appliance** and press Enter.

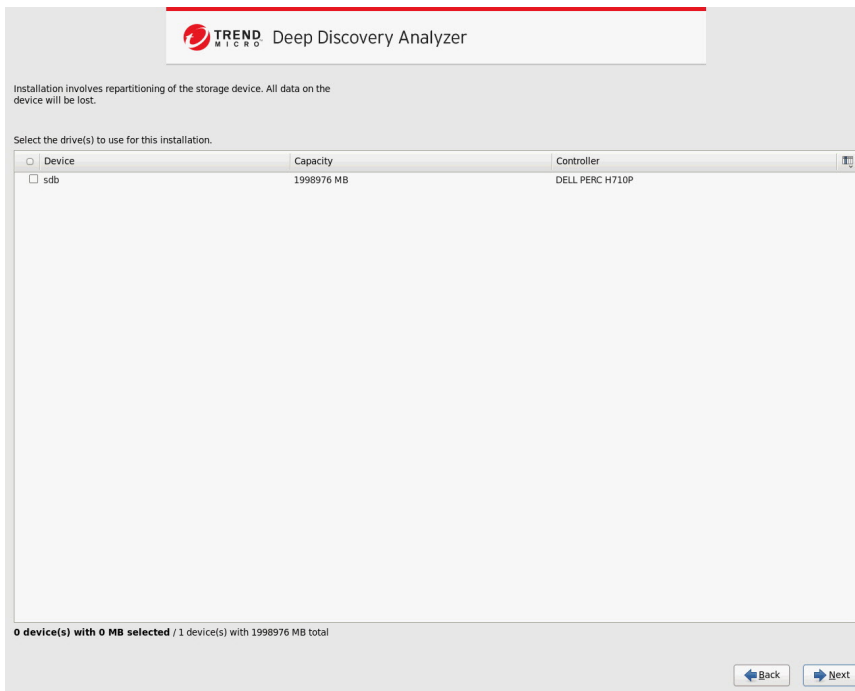
The **Welcome** screen appears.



The installation program checks for available installation media. If installation media is located, the **Trend Micro License Agreement** screen appears.

8. Click **Accept**.

The **Select Drive** screen appears.



9. Select at least one drive on which the Deep Discovery Analyzer software is installed.



WARNING!

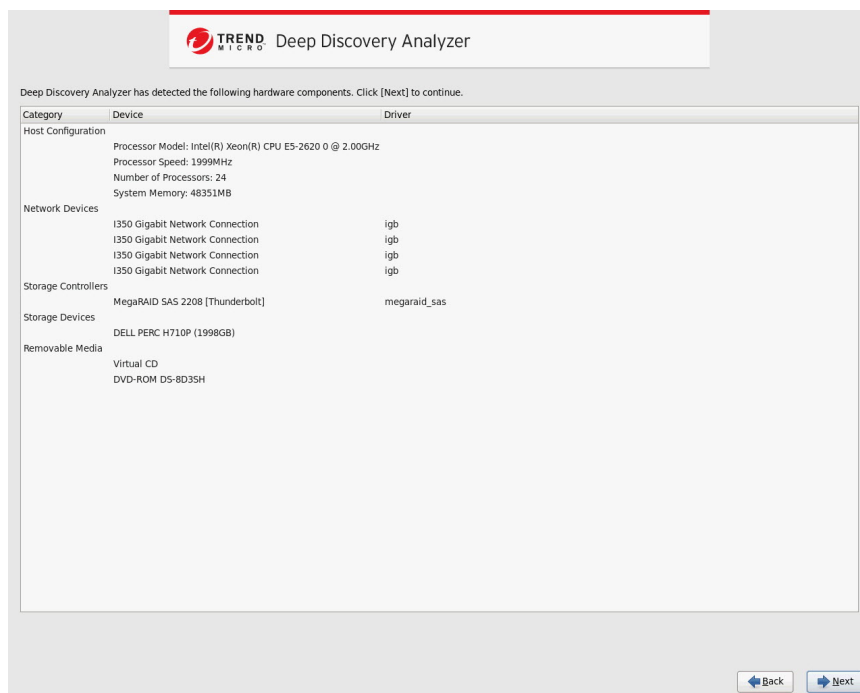
Installation involves repartitioning of the storage device. All data on the device is lost.

A confirmation message appears.



10. Click **Yes** to continue.

The program checks if the minimum hardware requirements are met, and then displays the hardware summary screen.



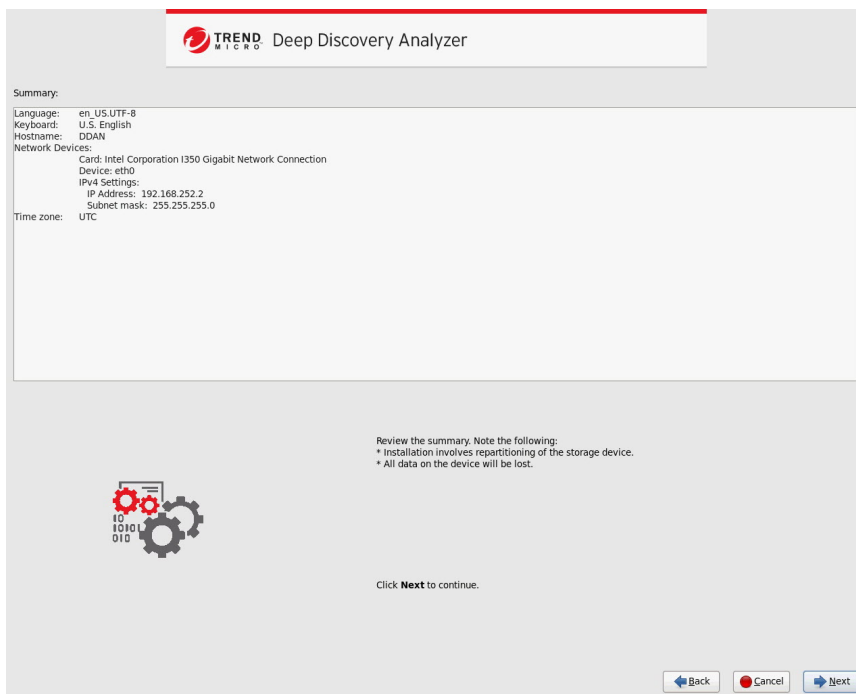
**Note**

Deep Discovery Analyzer requires at least:

- 8 GB RAM
- 400 GB available disk space
- At least two CPUs
- One Ethernet network interface card

11. Click **Next.**

The **Installation Summary** screen appears.

**12. Review the installation summary.**

**WARNING!**

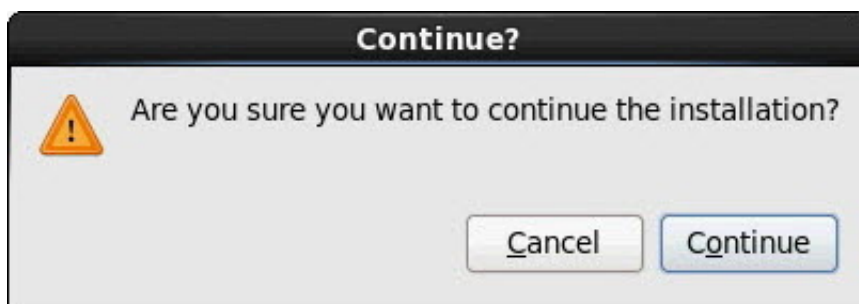
Installation involves repartitioning of the storage device.

All data on the storage device is lost.

You can change the host name, IP address, and date/time settings on the management console after all deployment tasks are completed. If you are unable to access the default IP address 192.168.252.2, use the preconfiguration console to modify the host name and IP address.

13. Click Next.

A confirmation message appears.



14. Click Continue.

The installation program formats the storage device and prepares the environment for installation. Upon completion, the appliance is restarted and the Deep Discovery Analyzer software is installed.

Chapter 3

Using the Preconfiguration Console

This chapter discusses how to use the Deep Discovery Analyzer preconfiguration console.

The Preconfiguration Console

The preconfiguration console is a Bash-based (Unix shell) interface used to configure network settings and ping remote hosts.

```

Main Menu
Configure Deep Discovery Analyzer.
(IPv4: 192.168.252.2 | IPv6: FE80::20C:29FF:FE54:D1F7)

1 Configure appliance IP address
2 Ping remote host
3 Change password
4 Log off

< Next >

```

The following table describes the tasks performed on the preconfiguration console.

TASK	PROCEDURE
Logging on	Type valid logon credentials. The default credentials are: <ul style="list-style-type: none"> User name: <code>admin</code> Password: <code>admin</code>
Configuring network addresses for the appliance	Specify the appliance IP address, subnet mask, gateway, and DNS. For details, see Configuring Network Addresses on the Preconfiguration Console on page 3-4 .
Pinging a remote host	Type a valid IP address or FQDN and click Ping .
Changing the preconfiguration console password	Type the new password twice and click Save .

TASK	PROCEDURE
Logging off	On the Main Menu , click Log off .







Preconfiguration Console Basic Operations


Use the following keyboard keys to perform basic operations on the preconfiguration console.



Important

Disable scroll lock (using the SCROLL LOCK key on the keyboard) to perform the following operations.

KEYBOARD KEY	OPERATION
<div>Up and Down arrows</div> <div> </div>	Move between fields.
	Move between items in a numbered list. <div><div> Note</div><div>An alternative way of moving to an item is by typing the item number.</div></div>
	Move between text boxes.
<div>Left and Right arrows</div> <div></div>	Move between buttons. Buttons are enclosed in angle brackets <>.
	Move between characters in a text box.
<div>ENTER</div> <div></div>	Click the highlighted item or button.

KEYBOARD KEY	OPERATION
TAB 	Move between screen sections, where one section requires using a combination of arrow keys (Up, Down, Left, and Right keys).

Configuring Network Addresses on the Preconfiguration Console

Procedure

1. Type valid logon credentials. The default credentials are:

- User name: `admin`
- Password: `admin`



Note

None of the characters you type appear on the screen.

This password is different from the password used to log on to the web-based management console. For more information, see [Logon Credentials on page 1-7](#).

The **Main Menu** screen appears.

```

Main Menu
Configure Deep Discovery Analyzer.
(IPv4: 192.168.252.2 | IPv6: FE80::28C:29FF:FE54:D1F7)

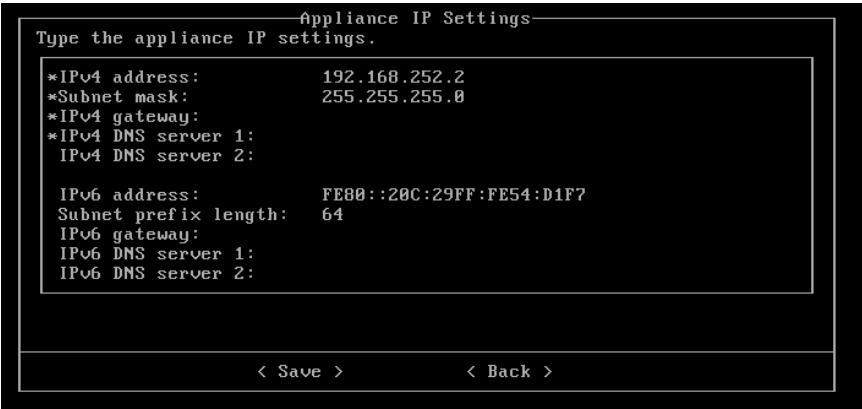
1 Configure appliance IP address
2 Ping remote host
3 Change password
4 Log off

< Next >


```

2. Select **Configure appliance IP address** and press ENTER.

The **Appliance IP Settings** screen appears.



3. Specify the following required settings:

ITEM	GUIDELINES
IPv4 address	<p>Must not conflict with the following addresses:</p> <ul style="list-style-type: none">Sandbox network: Configured in Virtual Analyzer > Sandbox Management > Network ConnectionVirtual Analyzer: 1.1.0.0 - 1.1.2.255Broadcast: 255.255.255.255Multicast: 224.0.0.0 - 239.255.255.255Link local: 169.254.1.0 - 169.254.254.255Class E: 240.0.0.0 - 255.255.255.255Localhost: 127.0.0.1/8 <hr/> <p> Note Changing the IP address changes the management console URL.</p>

ITEM	GUIDELINES
Subnet mask	Must not be any of the following addresses: <ul style="list-style-type: none">• 000.000.000.000• 111.111.111.111
IPv4 gateway	Must be in the same subnet as the IP address
IPv4 DNS server 1	Same as IP address
IPv4 DNS server 2 (Optional)	Same as IP address

4. (Optional) Configure the IPv6 settings.
5. Press TAB to navigate to **Save**, and then press ENTER.

The **Main Menu** screen appears after the settings are successfully saved.

Chapter 4

Migrating Deep Discovery Analyzer 5.0 to 5.1

This chapter discusses the tasks to migrate Deep Discovery Analyzer 5.0 to 5.1.

Most of the configuration settings and data can migrate from Deep Discovery Analyzer 5.0 to 5.1.

The following data can migrate.

- All submissions in **Virtual Analyzer > Submissions** that are completed, processing and queued
- All reports in **Reports > Generated Reports** and all schedules in **Reports > Report Settings**
- All suspicious objects in **Virtual Analyzer > Suspicious Objects**

The following settings cannot migrate.

- Tab settings in Dashboard
- Appliance IP settings
- License and Activation Code
- Sandbox network connection settings

Virtual Analyzer images imported in Deep Discovery Analyzer 5.0 cannot migrate.

Migration Tasks

This procedure outlines migrating the configuration settings and data from Deep Discovery Analyzer 5.0 to Deep Discovery Analyzer 5.1.

Procedure

1. Contact your support provider to obtain the Deep Discovery Analyzer 5.0 hot fix file (ddan_50_1x_en_hfb1080 or later) and the Deep Discovery Analyzer 5.1 installation ISO file.

2. Install the Deep Discovery Analyzer 5.0 hot fix.

For details, see the *Deep Discovery Analyzer 5.0 Administrator's Guide*.

3. Prepare the Samba server.

- a. (Windows 7 only) Modify the system registry on the Samba server.

For details, see [Preparing a Windows 7 Samba Server on page 4-4](#).

- b. Prepare the necessary disk space.

The necessary disk space appears on the **Export** screen. For details, see [Exporting Configuration Settings and Data on page 4-5](#).

4. Export the configuration settings and data from Deep Discovery Analyzer 5.0.

For details, see [Exporting Configuration Settings and Data on page 4-5](#).

5. Power off the Deep Discovery Analyzer 5.0 appliance.

For details, see the *Deep Discovery Analyzer 5.0 Administrator's Guide*.

6. Install Deep Discovery Analyzer 5.1.

For details, see [Installing Deep Discovery Analyzer on page 2-3](#).



Note

Deep Discovery Analyzer 5.1 can install on the Deep Discovery Analyzer 5.0 appliance hardware.

7. Configure a temporary IP address in the Deep Discovery Analyzer 5.1 preconfiguration console. Use a temporary IP address that is not the same as the Deep Discovery Analyzer 5.0 IP address.

For details, see [Configuring Network Addresses on the Preconfiguration Console on page 3-4](#).

8. Clear the browser cache.

For details, see [Clearing the Browser Cache on page 4-7](#).

9. Import the configuration settings and data to Deep Discovery Analyzer 5.1.

For details, see [Importing Configuration Settings and Data on page 4-6](#).

10. Perform the getting started tasks from Chapter 2 of the *Deep Discovery Analyzer 5.1 Administrator's Guide*.

**Note**

Trend Micro recommends using the same IP address as the Deep Discovery Analyzer 5.0 appliance.

11. Re-register all integrated products if the Deep Discovery Analyzer 5.1 appliance IP address is different than the Deep Discovery Analyzer 5.0 appliance IP address.

For details, see the documentation of the integrated product.

12. Update the components on Deep Discovery Analyzer 5.1.

For details, see the *Deep Discovery Analyzer 5.1 Administrator's Guide*.

13. (Optional) Restore the services on Deep Discovery Analyzer 5.0.

For details, see [Restoring Services After Migration on page 4-8](#).

Preparing a Windows 7 Samba Server

To prevent a "cannot allocate memory" error, perform the following procedure on the Windows 7 Samba server.

Procedure

1. Right-click the shared folder and select **Properties**. Allocate permissions on both the **Security** and the **Sharing** tabs for the Windows user.
 2. Open Registry Editor (regedit.exe).
 3. Set the value of the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache registry key to **1**.
 4. Set the value of the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size registry key to **3**.
 5. Restart the computer.
-

Exporting Configuration Settings and Data

Deep Discovery Analyzer 5.0 services stop after exporting the configuration settings and data. The exported data is inaccessible on Deep Discovery Analyzer 5.0.

Procedure

1. Go to <https://<Deep Discovery Analyzer 5.0 IP Address>/pages/rdqa.php>.
2. Verify the Samba server has enough disk space to accommodate the **Export size**.
3. Type the Samba server shared path, user name, and password.

The Samba shared path format is `\\<host name or IP address>\<shared path to data>`. For example, `\\192.168.2.34\data\export`.

4. Click **Export**.



Note

The export may take several minutes. Do not close the window or navigate to another page until the process completes.

The export was successfully completed appears on the screen and the Deep Discovery Analyzer 5.0 services are stopped.

✓ The export was successfully completed

Export

Export configuration and data to a Samba share. Ensure that the Samba share has enough space before proceeding.

Export size: 311.42 MB

Samba server shared path:

Samba server user name:

Samba server password:

Export

Recover services

Importing Configuration Settings and Data

Procedure

1. Go to <https://<Deep Discovery Analyzer 5.1 IP Address>/pages/rdqa.php>.
2. Click **Migration from Deep Discovery Analyzer 5.0**.
3. Type the Samba server shared path, user name, and password.

The Samba shared path format is `\\<host name or IP address>\<shared path to data>`. For example, `\\192.168.2.34\data\export`.

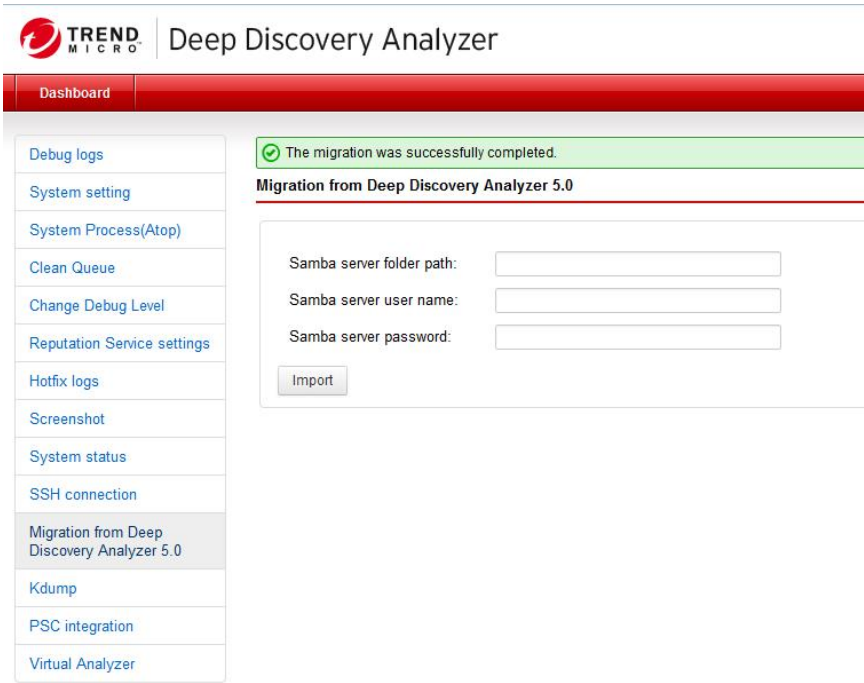
4. Click **Import**.



Note

The import may take several minutes. Do not close the window or navigate to another page until the process completes.

The migration was successfully completed appears.



Clearing the Browser Cache

Procedure

1. On Chrome™:
 - a. On the browser, go to **Settings**.

- b. Click **Show advanced settings...**
 - c. Under **Privacy**, click **Clear browsing data...**
 - d. Select **Cookies and other site and plug-in data** and **Cached images and files**.
 - e. Click **Clear browsing data**.
 - 2. On Internet Explorer®:
 - a. Go to **Tools > Internet Options > General**.
 - b. Under **Browsing history**, click **Delete**.

The **Delete Browsing History** window opens.
 - c. Select **Temporary Internet files and website files**, and **Cookies and Website data**.
 - d. Click **Delete**.

The **Delete Browsing History** window closes.
 - e. On the **Internet Options** window, click **OK**.
 - 3. On Mozilla Firefox®:
 - a. Go to **Options > Privacy**.
 - b. Click **clear your recent history**.
 - c. Select **Cookies** and **Cache**.
 - d. Click **Clear now**.
-

Restoring Services After Migration

Deep Discovery Analyzer 5.0 can continue operation after migrating the configuration settings and data.

After restoring services, you can perform another migration if you upgrade this Deep Discovery Analyzer appliance from 5.0 to 5.1.

**WARNING!**

All migrated data is inaccessible on Deep Discovery Analyzer 5.0.

Before restoring services, perform all migration tasks and verify the migrated data integrity on Deep Discovery Analyzer 5.1.

Procedure

1. Verify that the Deep Discovery Analyzer 5.0 appliance IP address is currently not in use by another device on the network.
 2. Power on the Deep Discovery Analyzer 5.0 appliance.
 3. Go to <https://<Deep Discovery Analyzer 5.0 IP Address>/pages/rdqa.php>.
 4. Click **Export**.
The **Export** screen appears.
 5. Click **Recover services**.
-

Chapter 5

Technical Support

Topics include:

- *Troubleshooting Resources on page 5-2*
- *Contacting Trend Micro on page 5-3*
- *Sending Suspicious Content to Trend Micro on page 5-5*
- *Other Resources on page 5-6*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Trend Community

To get help, share experiences, ask questions, and discuss security concerns with other users, enthusiasts, and security experts, go to:

<http://community.trendmicro.com/>

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 <http://esupport.trendmicro.com>.
2. Select a product or service from the appropriate drop-down list and specify any other related information.

The **Technical Support** product page appears.

3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

<http://esupport.trendmicro.com/srf/SRFMain.aspx>

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

Security Intelligence Community

Trend Micro cybersecurity experts are an elite security intelligence team specializing in threat detection and analysis, cloud and virtualization security, and data encryption.

Go to <http://www.trendmicro.com/us/security-intelligence/index.html> to learn about:

- Trend Micro blogs, Twitter, Facebook, YouTube, and other social media
- Threat reports, research papers, and spotlight articles
- Solutions, podcasts, and newsletters from global security insiders
- Free tools, apps, and widgets.

Threat Encyclopedia

Most malware today consists of “blended threats” - two or more technologies combined 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 <http://www.trendmicro.com/vinfo> 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.

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone, fax, or email:

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<http://docs.trendmicro.com>

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 hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

File Reputation Services

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

<http://esupport.trendmicro.com/solution/en-us/1059565.aspx>

Record the case number for tracking purposes.

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://ers.trendmicro.com/>

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

<http://esupport.trendmicro.com/solution/en-us/1036097.aspx>

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):

<http://global.sitesafety.trendmicro.com/>

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

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.

TrendEdge

Find information about unsupported, innovative techniques, tools, and best practices for Trend Micro products and services. The TrendEdge database contains numerous documents covering a wide range of topics for Trend Micro partners, employees, and other interested parties.

See the latest information added to TrendEdge at:

<http://trendedge.trendmicro.com/>

Download Center

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:

<http://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.

TrendLabs

TrendLabsSM is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

<http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs>

Index

C

- cluster deployment, 1-3
- community, 5-2
- custom network, 1-2
- custom port, 1-5

D

- deployment tasks
 - hardware setup, 2-2
 - installation, 2-6

E

- Ethernet cables, 1-6

F

- form factor, 1-2

I

- installation tasks, 2-2
- IP addresses (for product), 1-5

M

- management network, 1-2
- management port, 1-5

N

- network environment, 1-2

O

- online
 - community, 5-2

P

- port, 1-5
- power supply, 2-2
- preconfiguration console, 3-2
 - operations, 3-3

- product specifications, 1-2

S

- support
 - knowledge base, 5-2
 - resolve issues faster, 5-4
 - TrendLabs, 5-6

T

- TrendLabs, 5-6



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: APEM56867/150213