TREND MICRO™

6.8

TREND MICRO™ Deep Discovery™ Analyzer

Installation and Deployment Guide

Breakthrough Protection Against APTs and Targeted Attacks

Endpoint Security

Network Security

Protected Cloud

TREND MICRO SMART Protection Network™

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/en-us/enterprise/deep-discovery-analyzer.aspx

Document Part No.: APEM68831/191002

Release Date: December 2019

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

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

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 Analyzer 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

Preface

Chapter 1: Introduction

Chapter 2: Preparing to Deploy Deep Discovery Analyzer

Appendix A: Getting Started

Index

Preface

Preface

Welcome to the Trend Micro™ Deep Discovery™ Analyzer *Installation and Deployment 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	PDF documentation provided with the product or downloadable from the Trend Micro website. 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.
Installation and Deployment Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Analyzer, and using the Preconfiguration Console to set initial configurations and perform system tasks.
Syslog Content Mapping Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Analyzer.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Analyzer 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 Analyzer management console. The Online Help contains explanations of Deep Discovery Analyzer components and features, as well as procedures needed to configure Deep Discovery Analyzer.
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: http://esupport.trendmicro.com

View and download product documentation from the Trend Micro Online Help 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
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

Terminology

Terminology	Description
ActiveUpdate Server	Provides updates for product components, including pattern files. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server.

Terminology	Description
Active primary appliance	Clustered appliance with which all management tasks are performed. Retains all configuration settings and allocates submissions to secondary appliances for performance improvement.
Administrator	The person managing Deep Discovery Analyzer
Clustering	Multiple standalone Deep Discovery Analyzer appliances can be deployed and configured to form a cluster that provides fault tolerance, improved performance, or a combination thereof.
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
High availability cluster	In a high availability cluster, one appliance acts as the active primary appliance, and one acts as the passive primary appliance. The passive primary appliance automatically takes over as the new active primary appliance if the active primary appliance encounters an error and is unable to recover.
Load-balancing cluster	In a load-balancing cluster, one appliance acts as the active primary appliance, and any additional appliances act as secondary appliances. The secondary appliances process submissions allocated by the active primary appliance for performance improvement.
Management console	A web-based user interface for managing a product.
Management port	A hardware port that connects to the management network.
Passive primary appliance	Clustered appliance that is on standby until active primary appliance encounters an error and is unable to recover. Provides high availability.
Role-based administration	Role-based administration streamlines how administrators configure user accounts and control access to the management console.

Terminology	Description
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.
Secondary appliance	Clustered appliance that processes submissions allocated by the active primary appliance for performance improvement.
Standalone appliance	Appliance that is not part of any cluster. Clustered appliances can revert to being standalone appliances by detaching the appliance from its cluster.
Threat Connect	Correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network. The resulting intelligence reports enable you to investigate potential threats and take actions pertinent to your attack profile.
Virtual Analyzer	An isolated virtual environment used to manage and analyze samples. Virtual Analyzer observes sample behavior and characteristics, and then assigns a risk level to the sample.
Widget	A customizable screen to view targeted, selected data sets.
YARA	YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to your environment.

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

Introduction

This chapter introduces Deep Discovery Analyzer 6.8 and the new features in this release.

About Deep Discovery Analyzer

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 products. The custom sandboxing environments that can be created within Deep Discovery Analyzer precisely match target desktop software configurations — resulting in more accurate detections and fewer false positives.

Deep Discovery Analyzer also provides a Web Services API to allow integration with any third-party product, and a manual submission feature for threat research.

What's New

TABLE 1-1. What's New in Deep Discovery Analyzer 6.8

FEATURE/ENHANCEMENT	DETAILS
MITRE ATT&CK™ Framework Tactics and Techniques information	Deep Discovery Analyzer detection details and reports include MITRE ATT&CK™ Framework Tactics and Techniques information.

Feature/Enhancement	Details
Enhanced Virtual Analyzer	The internal Virtual Analyzer has been enhanced. This release adds the following features: • New Windows file types (.mht and .com) for sandbox analysis • Image support for Windows 10 RS4/RS5, Windows 10 LTSC • Windows editions with support for UEFI • Microsoft Office 2019 application support in Virtual Analyzer images • URL extraction from RTF files for analysis by Web Reputation Services This release also provides enhanced Virtual Analyzer management to allow you to: • Rename image groups • View actual Virtual Analyzer instance count on the Virtual Analyzer Status widget and the Sandbox Management screen
Enhanced detection capabilities	Deep Discovery Analyzer provides increased protection by improving its detection capabilities. This release includes the following features: • File password import and export • Support up to 100 file password entries
File SHA-256 support for user-defined suspicious objects	Deep Discovery Analyzer supports file SHA-256 user-defined suspicious object for the following: • Configuration through the management console or STIX file import • Synchronization from Deep Discovery Director • Sample analysis in ICAP pre-scan and Virtual Analyzer • Detection result display on the Submissions screen

Feature/Enhancement	Details
Enhanced ICAP integration	The Predictive Machine Learning engine has been enhanced to support macro and Executable and Linkable Format (ELF) file types for ICAP integration.
System proxy for component updates	Deep Discovery Analyzer provides the option to bypass the system proxy setting to connect to other update sources for component updates.
Enhanced Deep Discovery Director integration	Deep Discovery Director integration has been enhanced to enable the following: • Server port configuration for Deep Discovery Director communication • Up to 80K entries for user-defined suspicious object synchronization • Support Deep Discovery Director 5.1 integration for user-defined suspicious object expiration and central management of file passwords and file SHA-256 user-defined suspicious objects
Enhanced YARA rule feature	The enhanced YARA rule feature includes the following: • Dropped file information in detection result display on the Submissions screens • Support 3.10.0 of the official specifications
New integrated Trend Micro product	Deep Discovery Analyzer supports integration with Deep Discovery Web Inspector 2.5.
Enhanced management console	The management console has been enhanced to include the following: • Save custom column settings on Submissions screens for each user account • Automatic screen data reload upon switching Submissions screens
Inline migration from Deep Discovery Analyzer 6.1 and 6.5	Deep Discovery Analyzer can automatically migrate the settings of a Deep Discovery Analyzer 6.1 Patch 1 and 6.5 Patch 1 installation to 6.8.

Features and Benefits

Deep Discovery Analyzer includes the following features:

- *Enable Sandboxing as a Centralized Service on page 1-5*
- *Custom Sandboxing on page 1-5*
- *Broad File Analysis Range on page 1-6*
- *YARA Rules on page 1-6*
- *Document Exploit Detection on page 1-6*
- *Automatic URL Analysis on page 1-6*
- *Detailed Reporting on page 1-6*
- *Alert Notifications on page 1-6*
- *Clustered Deployment on page 1-7*
- *Trend Micro Product Integration on page 1-7*
- *Web Services API and Manual Submission on page 1-7*
- *Custom Defense Integration on page 1-7*
- *ICAP Integration on page 1-7*

Enable Sandboxing as a Centralized Service

Deep Discovery Analyzer ensures optimized performance with a scalable solution able to keep pace with email, network, endpoint, and any additional source of samples.

Custom Sandboxing

Deep Discovery Analyzer performs sandbox simulation and analysis in environments that match the desktop software configurations attackers expect in your environment and ensures optimal detection with low false-positive rates.

Broad File Analysis Range

Deep Discovery Analyzer examines a wide range of Windows executable, Microsoft Office, PDF, web content, and compressed file types using multiple detection engines and sandboxing.

YARA Rules

Deep Discovery Analyzer uses YARA rules to identify malware. YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to your environment.

Document Exploit Detection

Using specialized detection and sandboxing, Deep Discovery Analyzer discovers malware and exploits that are often delivered in common office documents and other file formats.

Automatic URL Analysis

Deep Discovery Analyzer performs page scanning and sandbox analysis of URLs that are automatically submitted by integrating products.

Detailed Reporting

Deep Discovery Analyzer delivers full analysis results including detailed sample activities and C&C communications via central dashboards and reports.

Alert Notifications

Alert notifications provide immediate intelligence about the state of Deep Discovery Analyzer.

Clustered Deployment

Multiple standalone Deep Discovery Analyzer appliances can be deployed and configured to form a cluster that provides fault tolerance, improved performance, or a combination thereof.

Trend Micro Product Integration

Deep Discovery Analyzer enables out-of-the-box integration to expand the sandboxing capacity of Trend Micro email and web security products.

Web Services API and Manual Submission

Deep Discovery Analyzer allows any security product or authorized threat researcher to submit samples.

Custom Defense Integration

Deep Discovery Analyzer shares new IOC detection intelligence automatically with other Trend Micro solutions and third-party security products.

ICAP Integration

Deep Discovery Analyzer supports integration with Internet Content Adaptation Protocol (ICAP) clients. After integration, Deep Discovery Analyzer can perform the following functions:

- Work as an ICAP server that analyzes samples submitted by ICAP clients
- Serve User Configuration Pages to the end user when the specified network behavior (URL access / file upload / file download) is blocked
- Control which ICAP clients can submit samples by configuring the ICAP Client list
- Bypass file scanning based on selected MIME content-types

- Bypass file scanning based on true file types
- Bypass URL scanning in RESPMOD mode
- Scan samples using different scanning modules
- Filter sample submissions based on the file types that Virtual Analyzer can process.

Chapter 2

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 or hotfix to apply to it, see the *Deep Discovery Analyzer Administrator's Guide*.

Deployment Overview

Product Specifications

Standard Deep Discovery Analyzer appliances have the following specifications.

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

Product Specifications - 1000 Appliance

Feature	Specifications
Rack size	2U 19-inch standard rack
Availability	Raid 5 configuration
Storage size	2 TB free storage
Connectivity	• 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

Product Specifications - 1100 Appliance

Feature	Specifications
Rack size	2U 19-inch standard rack
Availability	Raid 1 configuration

FEATURE	SPECIFICATIONS
Storage size	4 TB free storage
Connectivity	• 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	31.5 kg (69.45 lb)
Operating temperature	10 °C to 35 °C at 10% to 80% relative humidity (RH)
Power	750W, 120-240 VAC 50/60 Hz

Product Specifications - 1200 Appliance

FEATURE	SPECIFICATIONS
Rack size	2U 19-inch standard rack
Availability	Raid 1 configuration
Storage size	4 TB free storage
Connectivity	• 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 75.13cm (29.58 in) x 8.68 cm (3.42 in)
Maximum weight	28.6 kg (63.05 lb)
Operating temperature	10 °C to 35 °C at 10% to 80% relative humidity (RH)
Power	750W , 120-240 VAC 50/60 Hz

Deployment Considerations

Any Deep Discovery Analyzer appliance can be deployed and configured as a standalone appliance. A standalone appliance processes all submitted objects without the assistance of other Deep Discovery Analyzer appliances. It cannot provide continued scanning and analysis services when it encounters an error and is unable to recover.

Multiple standalone Deep Discovery Analyzer appliances can be deployed and configured to form a cluster that provides fault tolerance, improved performance, or a combination thereof.

Depending on your requirements and the number of Deep Discovery Analyzer appliances available, you may deploy the following cluster configurations:

TABLE 2-1. Cluster Configurations

CLUSTER CONFIGURATION	DESCRIPTION
High availability cluster	In a high availability cluster, one appliance acts as the active primary appliance, and one acts as the passive primary appliance. The passive primary appliance automatically takes over as the new active primary appliance if the active primary appliance encounters an error and is unable to recover. For details, see *High Availability Cluster on page 2-5*.
Load-balancing cluster	In a load-balancing cluster, one appliance acts as the active primary appliance, and any additional appliances act as secondary appliances. The secondary appliances process submissions allocated by the active primary appliance for performance improvement. For details, see *Load-Balancing Cluster on page 2-6*.
High availability cluster with load balancing	In a high availability cluster with load balancing, one appliance acts as the active primary appliance, one acts as the passive primary appliance, and any additional appliances act as secondary appliances. The passive primary appliance takes over as the active primary appliance if the active primary appliance encounters an error and is unable to recover. The secondary appliances process submissions allocated by the active primary appliance for performance improvement. For details, see *High Availability Cluster with Load Balancing on page 2-7*.

High Availability Cluster

In a high availability cluster, one appliance acts as the active primary appliance, and one acts as the passive primary appliance. The passive primary appliance automatically takes over as the new active primary appliance if the active primary appliance encounters an error and is unable to recover.

Deploy this cluster configuration if you want to ensure that Deep Discovery Analyzer capabilities remain available even when the appliance encounters an error and is unable to recover.

The following figure shows two Deep Discovery Analyzer appliances deployed in a high availability cluster configuration and how integrating products communicate with Deep Discovery Analyzer.

Note

- Trend Micro recommends updating the firmware on a Deep Discovery Analyzer appliance to the latest version before deployment in a high availability cluster.
- The active primary appliance and the passive primary appliance must be connected using eth3.
- Trend Micro recommends using a Category 6 or higher Ethernet cable to directly connect the active primary appliance and passive primary appliance using eth3.
- Trend Micro recommends directly connecting the active primary appliance and the passive primary appliance to minimize potential points of failures.
- If the active primary appliance is not connected to the passive primary appliance directly (for example, if they are in different data centers), the following requirements must be met:
    - The appliances must be Deep Discovery Analyzer 1100 or 1200
    - The connections between the appliances must meet the following conditions:
        - Network latency is less than 15 ms
        - Packet loss ratio is less than 0.000001%
        - Network bandwidth is greater than 240Mbps

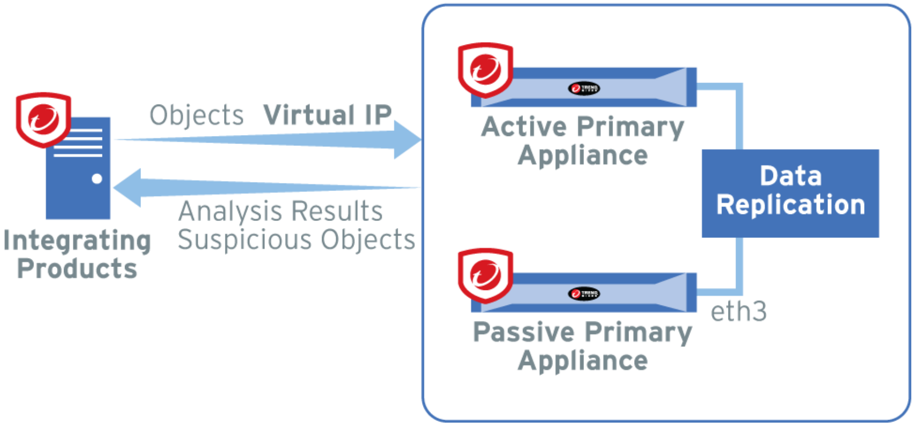


FIGURE 2-1. High Availability Cluster

Load-Balancing Cluster

In a load-balancing cluster, one appliance acts as the active primary appliance, and any additional appliances act as secondary appliances. The secondary appliances process submissions allocated by the active primary appliance for performance improvement.

Deploy this cluster configuration if you require improved object processing performance.

The following figure shows Deep Discovery Analyzer appliances deployed in a load-balancing cluster configuration and how integrating products communicate with Deep Discovery Analyzer.

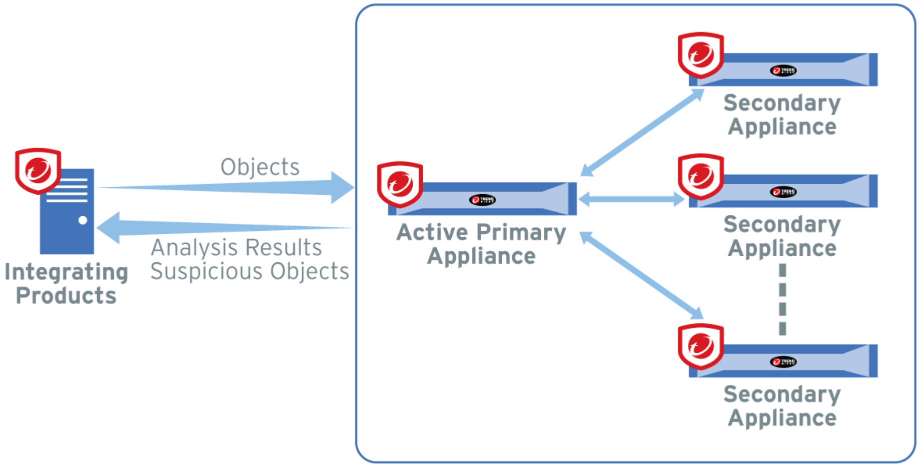


FIGURE 2-2. Load-Balancing Cluster

High Availability Cluster with Load Balancing

In a high availability cluster with load balancing, one appliance acts as the active primary appliance, one acts as the passive primary appliance, and any additional appliances act as secondary appliances. The passive primary appliance takes over as the active primary appliance if the active primary appliance encounters an error and is unable to recover. The secondary appliances process submissions allocated by the active primary appliance for performance improvement.

Deploy this cluster configuration if you want to combine the benefits of high availability clustering and load-balancing clustering.

The following figure shows Deep Discovery Analyzer appliances deployed in a high availability cluster configuration and how integrating products communicate with Deep Discovery Analyzer.

Note

- Trend Micro recommends updating the firmware on a Deep Discovery Analyzer appliance to the latest version before deployment in a high availability cluster.
- The active primary appliance and the passive primary appliance must be connected using eth3.
- Trend Micro recommends using a Category 6 or higher Ethernet cable to directly connect the active primary appliance and passive primary appliance using eth3.
- Trend Micro recommends directly connecting the active primary appliance and the passive primary appliance to minimize potential points of failures.
- If the active primary appliance is not connected to the passive primary appliance directly (for example, if they are in different data centers), the following requirements must be met:
    - The appliances must be Deep Discovery Analyzer 1100 or 1200
    - The connections between the appliances must meet the following conditions:
        - Network latency is less than 15 ms
        - Packet loss ratio is less than 0.000001%
        - Network bandwidth is greater than 240Mbps

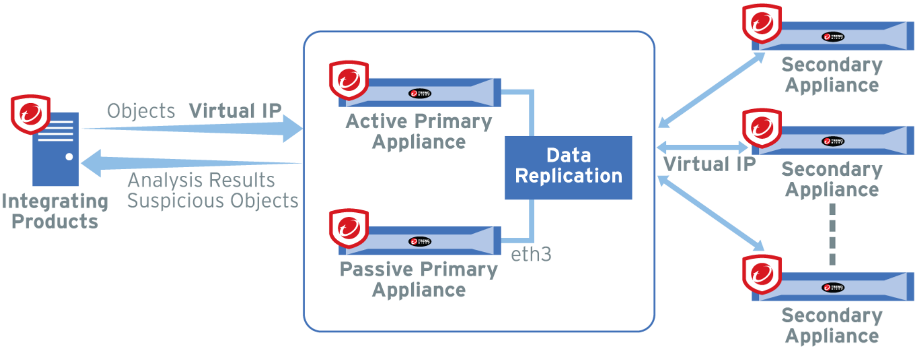
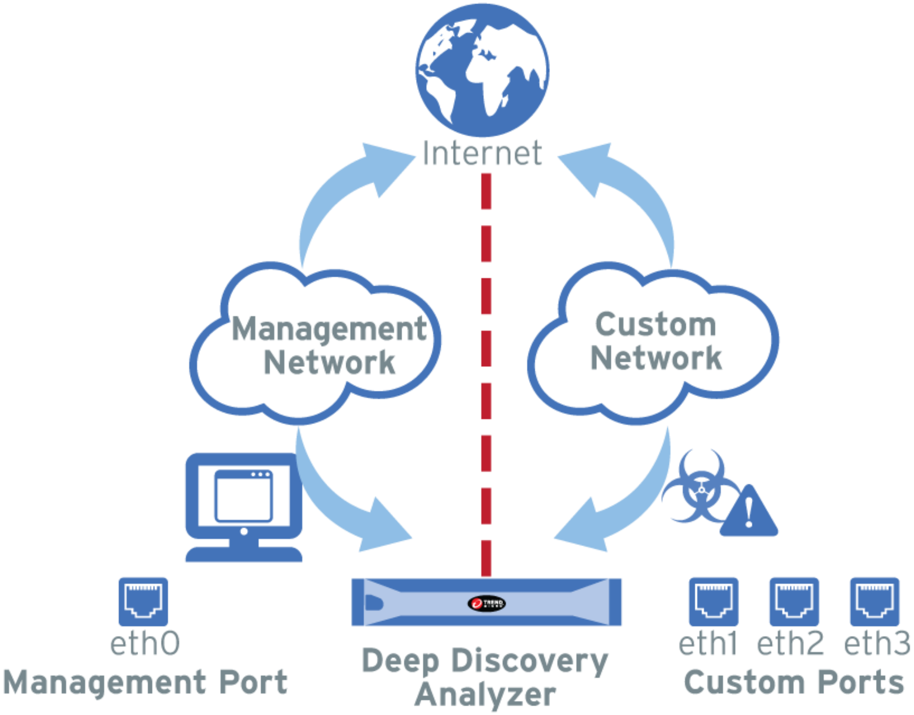


FIGURE 2-3. High Availability Cluster with Load Balancing

Recommended Network Environment

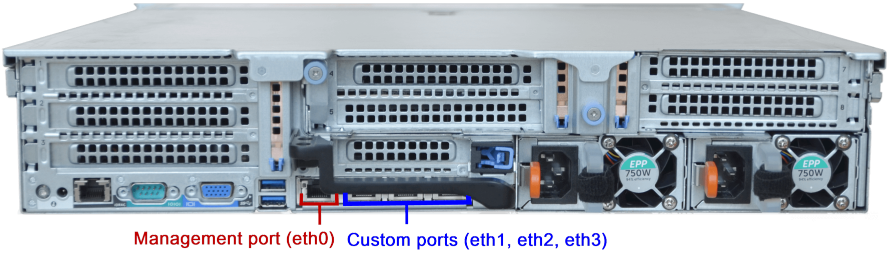
Deep Discovery Analyzer requires connection to a management network, which usually is the organization's intranet. After deployment, administrators can perform configuration tasks from any computer on the management network.

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.



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

Note

- Only of the interfaces, eth1, eth2, or eth3, can be used for sandbox analysis.
- When using high availability, eth3 is used to directly connect two identical appliances and cannot be used 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 addresses. For more information, see the *Deep Discovery Analyzer Administrator's Guide*.

Deployment Requirements

Requirement	Details
Deep Discovery Analyzer	Obtain from Trend Micro
Deep Discovery Analyzer installation CD	Obtain from Trend Micro
Activation Code	Obtain from Trend Micro
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	• 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. • If using high availability, one cable connects eth3 to eth3 on an identical appliance.
IP addresses	• One static IP address in the management network • If sandbox instances require Internet connectivity, one extra IP address for Virtual Analyzer • If using high availability, one extra virtual IP address
Software	Any of the following browsers: • Microsoft Internet Explorer™ 9, 10, or 11 • Microsoft Edge™ • Google Chrome™ • Mozilla Firefox™
Third-party software licenses	Licenses for all third-party software installed on sandbox images

Requirement	Details
Pre-requisites for product integration	If integrating with another product, verify that all integration requirements have been met. • Some integrating products require additional configuration (for example: host names, IP addresses, SSL ports, etc) to integrate with Deep Discovery Analyzer properly. See the product documentation for details. • Some integrating products require an API key provided by Deep Discovery Analyzer. If the Deep Discovery Analyzer API key changes after registering with the integrated product, remove Deep Discovery Analyzer from the integrated product and add it again. • Internet Content Adaptation Protocol (ICAP) clients must comply with RFC 3507.

Logon Credentials

Console	Purpose	Default Credentials	Your Information
Preconfiguration console	Perform initial configuration tasks. See *Configuring Network Addresses on the Preconfiguration Console on page 4-5*.	• Deep Discovery Analyzer **login** (not configurable) : `admin` • **Password**: `Admin1234!`	**Password**:

Console	Purpose	Default Credentials	Your Information
Management console	• Configure product settings • View and download reports	• **User name** (not configurable): `admin` • **Password**: `Admin1234!`	**Password**:
		Other user accounts (configured on the management console, in **Administration** > **Accounts / Contacts** > **Accounts**)	User account 1: **User name**: **Password**:
			User account 2: **User name**: **Password**:

Ports Used by the Appliance

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

Table 2-2. Ports used by Deep Discovery Analyzer

Port	Protocol	Function	Purpose
21	TCP	Outbound	Deep Discovery Analyzer uses this port to send backup data to FTP servers.
22	TCP	Listening and outbound	Deep Discovery Analyzer uses this port to: • Access the preconfiguration console with a computer through SSH • Send backup data to an SFTP server • Send debug logs to an SFTP server

Port	Protocol	Function	Purpose
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	Listening	Deep Discovery Analyzer receives responses from the DHCP server.
80	TCP	Listening	Deep Discovery Analyzer uses this port to share suspicious object lists with third-party products.
123	UDP	Listening and outbound	Deep Discovery Analyzer connects to the NTP server to synchronize time.
137	UDP	Outbound	Deep Discovery Analyzer uses NetBIOS to resolve IP addresses to host names.
161	UDP	Listening	Deep Discovery Analyzer uses this port to listen for requests from SNMP managers.
162	UDP	Outbound	Deep Discovery Analyzer uses this port to send trap messages to SNMP managers.
443	TCP	Listening	Deep Discovery Analyzer uses this port to: • Access the management console with a computer through HTTPS • Communicate with other Deep Discovery Analyzer appliances in a cluster environment • Communicate with Trend Micro Apex Central • Receive files from a computer via the Manual Submission Tool • Receive samples from integrated products

Port	Protocol	Function	Purpose
			• Send Suspicious Objects list and analysis information to integrated products
		Outbound	Deep Discovery Analyzer uses this port to: • Connect to Trend Micro Threat Connect • Connect to Web Reputation Services to query the blocking reason • Connect to Sandbox as a Service for analysis of samples related to Mac OS • Connect to the Predictive Machine Learning engine • Update components by connecting to the ActiveUpdate server • Verify the safety of files through the Certified Safe Software Service • Communicate with Deep Discovery Director • Verify the Deep Discovery Analyzer product license through Customer Licensing Portal • Query Web Reputation Services through the Smart Protection Network • Connect to the Community File Reputation service for file prevalence when analyzing file samples • Connect to the Community Domain/IP Reputation service • Verify the Deep Discovery Analyzer product license through Customer Licensing Portal • Connect to Dynamic URL Scanning

Port	Protocol	Function	Purpose
User-defined		Listening	Deep Discovery Analyzer uses this user-defined port to: • Receive samples from ICAP clients using the ICAP protocol
		Outbound	Deep Discovery Analyzer uses user-defined ports to: • Send logs to syslog servers • Connect to proxy servers • Connect to the Smart Protection Server • Connect to Microsoft Active Directory servers • Send notifications and scheduled reports through SMTP

Chapter 3

Installing the Appliance

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 3-2*.

2. Install Deep Discovery Analyzer. For details, see *Installing Deep Discovery Analyzer on page 3-4*.

3. Configure the IP address of the appliance on the preconfiguration console. For details, see *Configuring Network Addresses on the Preconfiguration Console on page 4-5*.

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.

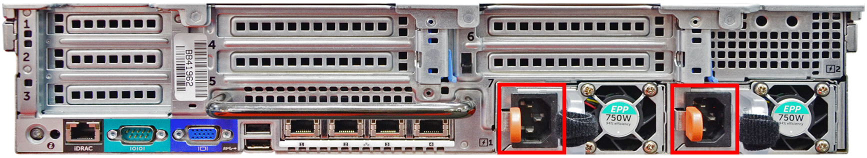


FIGURE 3-1. 1100 appliance AC power slots

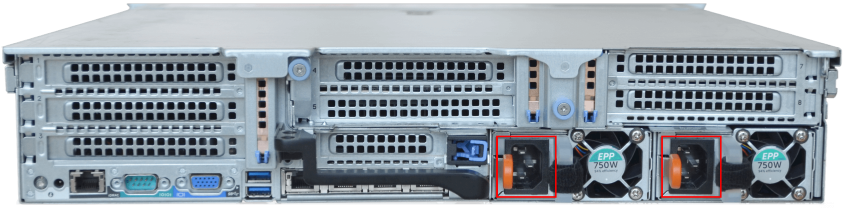


FIGURE 3-2. 1200 appliance AC power slots

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 the appliance to the management network

   - **Custom port**: A hardware port that connects the appliance to an isolated network dedicated to sandbox analysis

> **Note**
>
> When using high availability, eth3 is used to connect the two identical appliances and cannot be used for sandbox analysis.

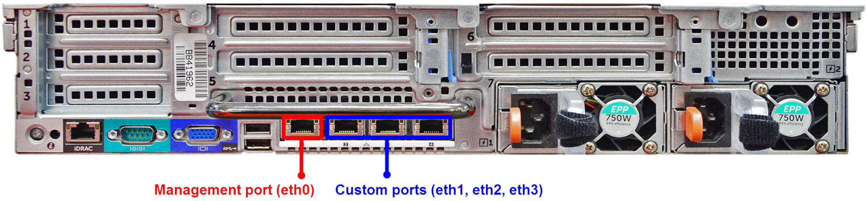


FIGURE 3-3. 1100 appliance ports

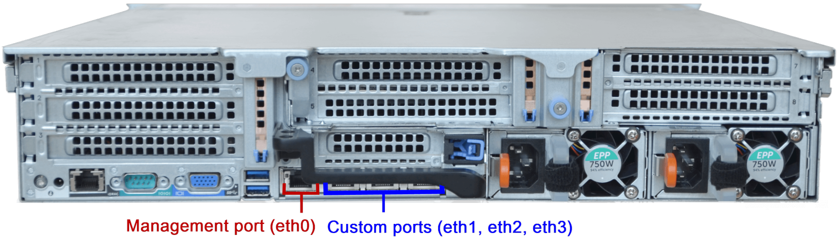


FIGURE 3-4. 1200 appliance ports

6. Power on the appliance.

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

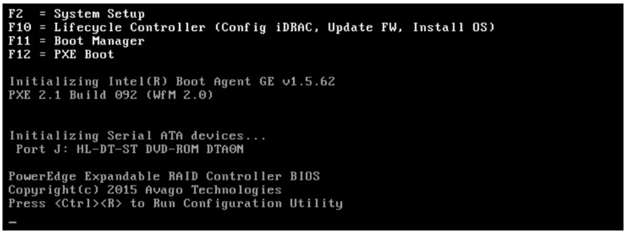
Installing Deep Discovery Analyzer

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.

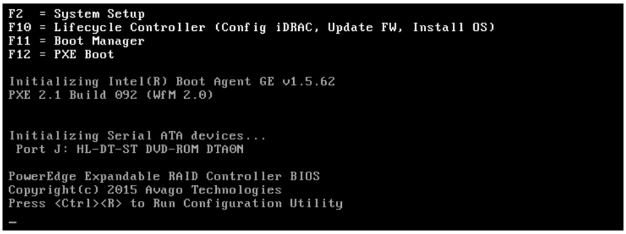


```
F2  = System Setup
F10 = Lifecycle Controller (Config iDRAC, Update FW, Install OS)
F11 = Boot Manager
F12 = PXE Boot

Initializing Intel(R) Boot Agent GE v1.5.62
PXE 2.1 Build 092 (WfM 2.0)


Initializing Serial ATA devices...
 Port J: HL-DT-ST DVD-ROM DTA0N

PowerEdge Expandable RAID Controller BIOS
Copyright(c) 2015 Avago Technologies
Press <Ctrl><R> to Run Configuration Utility
_
```

2. Insert the CD containing the Deep Discovery Analyzer installation package.

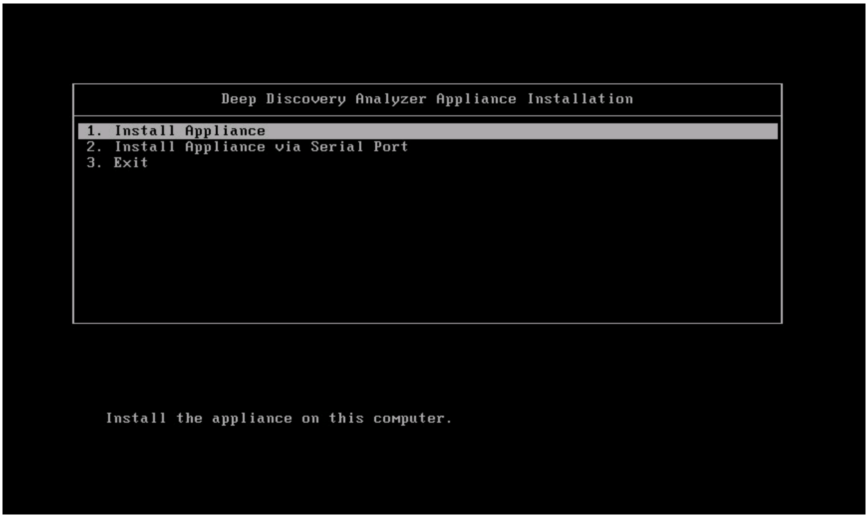
3. Restart the appliance.

   The **POST** screen appears.



```
F2  = System Setup
F10 = Lifecycle Controller (Config iDRAC, Update FW, Install OS)
F11 = Boot Manager
F12 = PXE Boot

Initializing Intel(R) Boot Agent GE v1.5.62
PXE 2.1 Build 092 (WfM 2.0)


Initializing Serial ATA devices...
 Port J: HL-DT-ST DVD-ROM DTA0N

PowerEdge Expandable RAID Controller BIOS
Copyright(c) 2015 Avago Technologies
Press <Ctrl><R> to Run Configuration Utility
_
```

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

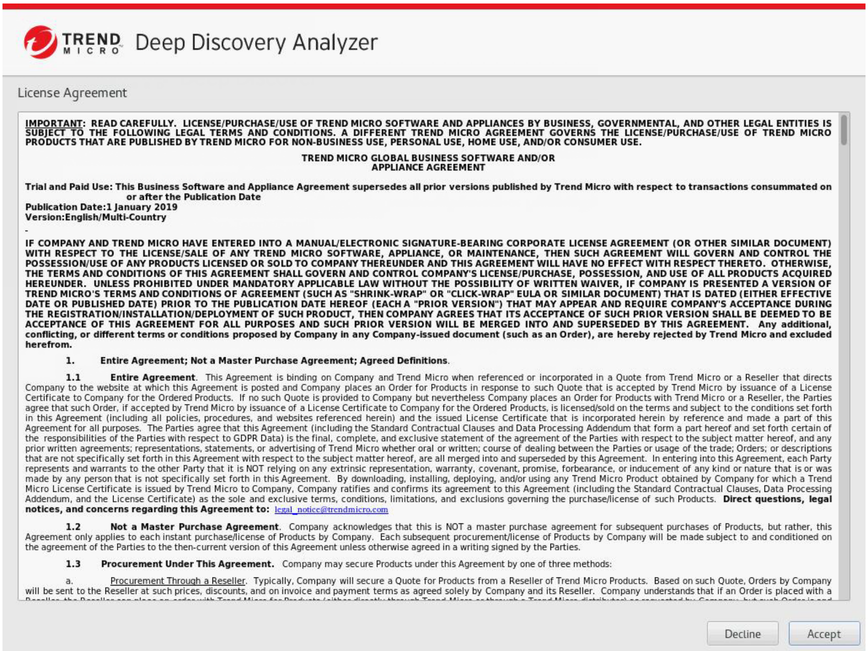


```
Deep Discovery Analyzer Appliance Installation

1. Install Appliance
2. Install Appliance via Serial Port
3. Exit




Install the appliance on this computer.
```

5. Select **1. Install Appliance** and press ENTER.

    - When installing Deep Discovery Analyzer via serial port, select **2. Install Appliance via Serial Port** and press ENTER.

The **License Agreement** screen appears.



IMPORTANT: READ CAREFULLY. LICENSE/PURCHASE/USE OF TREND MICRO SOFTWARE AND APPLIANCES BY BUSINESS, GOVERNMENTAL, AND OTHER LEGAL ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS. A DIFFERENT TREND MICRO AGREEMENT GOVERNS THE LICENSE/PURCHASE/USE OF TREND MICRO PRODUCTS THAT ARE PUBLISHED BY TREND MICRO FOR NON-BUSINESS USE, PERSONAL USE, HOME USE, AND/OR CONSUMER USE.

TRENDMICRO GLOBAL BUSINESS SOFTWARE AND/OR APPLIANCE AGREEMENT

Trial and Paid Use: This Business Software and Appliance Agreement supersedes all prior versions published by Trend Micro with respect to transactions consummated on or after the Publication Date
Publication Date:1 January 2019
Version:English/Multi-Country

-

IF COMPANY AND TREND MICRO HAVE ENTERED INTO A MANUAL/ELECTRONIC SIGNATURE-BEARING CORPORATE LICENSE AGREEMENT (OR OTHER SIMILAR DOCUMENT) WITH RESPECT TO THE LICENSE/SALE OF ANY TREND MICRO SOFTWARE, APPLIANCE, OR MAINTENANCE, THEN SUCH AGREEMENT WILL GOVERN AND CONTROL THE POSSESSION/USE OF ANY PRODUCTS LICENSED OR SOLD TO COMPANY THEREUNDER AND THIS AGREEMENT WILL HAVE NO EFFECT WITH RESPECT THERETO. OTHERWISE, THE TERMS AND CONDITIONS OF THIS AGREEMENT SHALL GOVERN AND CONTROL COMPANY'S LICENSE/PURCHASE, POSSESSION, AND USE OF ALL PRODUCTS ACQUIRED HEREUNDER. UNLESS PROHIBITED UNDER MANDATORY APPLICABLE LAW WITHOUT THE POSSIBILITY OF WRITTEN WAIVER, IF COMPANY IS PRESENTED A VERSION OF TREND MICRO'S TERMS AND CONDITIONS OF AGREEMENT (SUCH AS "SHRINK-WRAP" OR "CLICK-WRAP" EULA OR SIMILAR DOCUMENT) THAT IS DATED (EITHER EFFECTIVE DATE OR PUBLISHED DATE) PRIOR TO THE PUBLICATION DATE HEREOF (EACH A "PRIOR VERSION") THAT MAY APPEAR AND REQUIRE COMPANY'S ACCEPTANCE DURING THE REGISTRATION/INSTALLATION/DEPLOYMENT OF SUCH PRODUCT, THEN COMPANY AGREES THAT ITS ACCEPTANCE OF SUCH PRIOR VERSION SHALL BE DEEMED TO BE ACCEPTANCE OF THIS AGREEMENT FOR ALL PURPOSES AND SUCH PRIOR VERSION WILL BE MERGED INTO AND SUPERSEDED BY THIS AGREEMENT. Any additional, conflicting, or different terms or conditions proposed by Company in any Company-issued document (such as an Order), are hereby rejected by Trend Micro and excluded herefrom.

1. Entire Agreement; Not a Master Purchase Agreement; Agreed Definitions.

1.1 Entire Agreement. This Agreement is binding on Company and Trend Micro when referenced or incorporated in a Quote from Trend Micro or a Reseller that directs Company to the website at which this Agreement is posted and Company places an Order for Products in response to such Quote that is accepted by Trend Micro by issuance of a License Certificate to Company for the Ordered Products. If no such Quote is provided to Company but nevertheless Company places an Order for Products with Trend Micro or a Reseller, the Parties agree that such Order, if accepted by Trend Micro by issuance of a License Certificate to Company for the Ordered Products, is licensed/sold on the terms and subject to the conditions set forth in this Agreement (including all policies, procedures, and websites referenced herein) and the issued License Certificate that is incorporated herein by reference and made a part of this Agreement for all purposes. The Parties agree that this Agreement (including the Standard Contractual Clauses and Data Processing Addendum that form a part hereof and set forth certain of the responsibilities of the Parties with respect to GDPR Data) is the final, complete, and exclusive statement of the agreement of the Parties with respect to the subject matter hereof, and any prior written agreements; representations, statements, or advertising of Trend Micro whether oral or written; course of dealing between the Parties or usage of the trade; Orders; or descriptions that are not specifically set forth in this Agreement with respect to the subject matter hereof, are all merged into and superseded by this Agreement. In entering into this Agreement, each Party represents and warrants to the other Party that it is NOT relying on any extrinsic representation, warranty, covenant, promise, forbearance, or inducement of any kind or nature that is or was made by any person that is not specifically set forth in this Agreement. By downloading, installing, deploying, and/or using any Trend Micro Product obtained by Company for which a Trend Micro License Certificate is issued by Trend Micro to Company, Company ratifies and confirms its agreement to this Agreement (including the Standard Contractual Clauses, Data Processing Addendum, and the License Certificate) as the sole and exclusive terms, conditions, limitations, and exclusions governing the purchase/license of such Products. **Direct questions, legal notices, and concerns regarding this Agreement to:** legal_notice@trendmicro.com

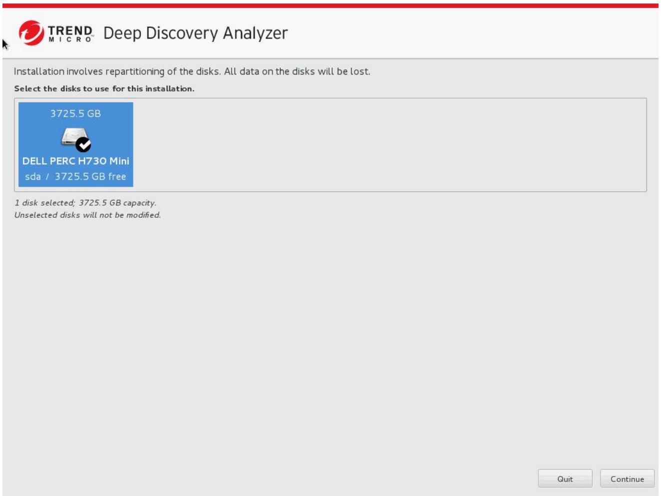
1.2 Not a Master Purchase Agreement. Company acknowledges that this is NOT a master purchase agreement for subsequent purchases of Products, but rather, this Agreement only applies to each instant purchase/license of Products by Company. Each subsequent procurement/license of Products by Company will be made subject to and conditioned on the agreement of the Parties to the then-current version of this Agreement unless otherwise agreed in a writing signed by the Parties.

1.3 Procurement Under This Agreement. Company may secure Products under this Agreement by one of three methods:

a. Procurement Through a Reseller. Typically, Company will secure a Quote for Products from a Reseller of Trend Micro Products. Based on such Quote, Orders by Company will be sent to the Reseller at such prices, discounts, and on invoice and payment terms as agreed solely by Company and its Reseller. Company understands that if an Order is placed with a

6. Click **Accept**.

The **Select Disk** screen appears.



Installation involves repartitioning of the disks. All data on the disks will be lost.

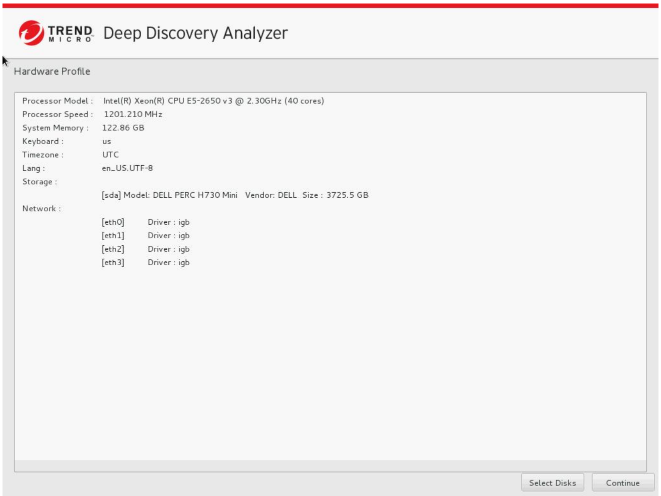
Select the disks to use for this installation.

1 disk selected; 3725.5 GB capacity.
Unselected disks will not be modified.

7. Select the disk on which to install the Deep Discovery Analyzer software.

8. Click **Continue**.

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



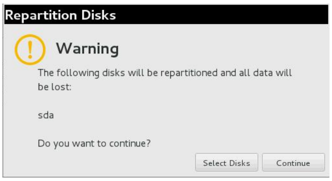
```
Processor Model :  Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz (40 cores)
Processor Speed :  1201.210 MHz
System Memory :    122.86 GB
Keyboard :         us
Timezone :         UTC
Lang :             en_US.UTF-8
Storage :
                   [sda] Model: DELL PERC H730 Mini   Vendor: DELL  Size : 3725.5 GB
Network :
                   [eth0]      Driver : igb
                   [eth1]      Driver : igb
                   [eth2]      Driver : igb
                   [eth3]      Driver : igb
```

9. Click **Continue**.

WARNING!

Installation involves repartitioning of the disks. All data on the disks are lost.

A confirmation message appears.



The following disks will be repartitioned and all data will be lost:

sda

Do you want to continue?

10. Click **Continue**.

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

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 4-5*.

Chapter 4

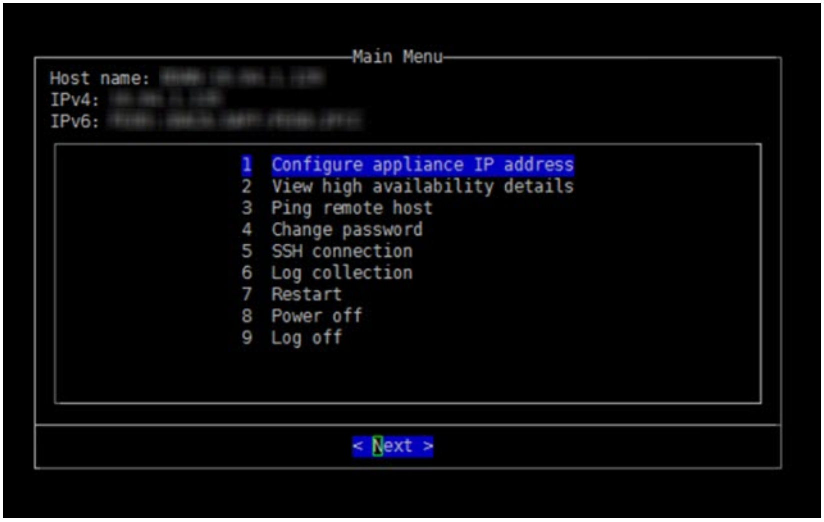
Using the Preconfiguration Console

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 that allows you to perform the following:

- Configure network settings
- View high availability details
- Test connection to remote hosts using ping
- Collect and upload debug logs
- Change the preconfiguration console password
- Restart or shut down the appliance



```
                              Main Menu
Host name: [redacted]
IPv4: [redacted]
IPv6: [redacted]

                 1  Configure appliance IP address
                 2  View high availability details
                 3  Ping remote host
                 4  Change password
                 5  SSH connection
                 6  Log collection
                 7  Restart
                 8  Power off
                 9  Log off

                              < Next >
```

The following table describes the tasks you can perform on the preconfiguration console.

Task	Procedure
Logging on	Type valid logon credentials. The default credentials are: • User name: `admin` • Password: `Admin1234!`
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 4-5*.
Viewing high availability details	View the active and passive appliance host names, IP addresses, and sync status. **Note** High availability cannot be configured on the preconfiguration console. Use the management console to configure high availability. For details see the *High Availability Tab* and *Cluster Tab* topics in the *Deep Discovery Analyzer Administrator's Guide*.
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 select **Save**.
Enabling and disabling SSH connection	Enabling or disabling the SSH connection.
Collecting and uploading debug logs	Collect debug logs from Deep Discovery Analyzer and upload debug logs to the SFTP server.
Restarting	On the **Main Menu**, select **Restart**, and press ENTER. On the next screen, select **OK** and press ENTER.
Powering off	On the **Main Menu**, select **Power off**, and press ENTER. On the next screen, select **OK** and press ENTER.

Task	Procedure
Logging off	On the **Main Menu**, select **Log off**, and press ENTER. On the next screen, select **OK** and press ENTER.

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

KEYBOARD KEY	OPERATION
TAB 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

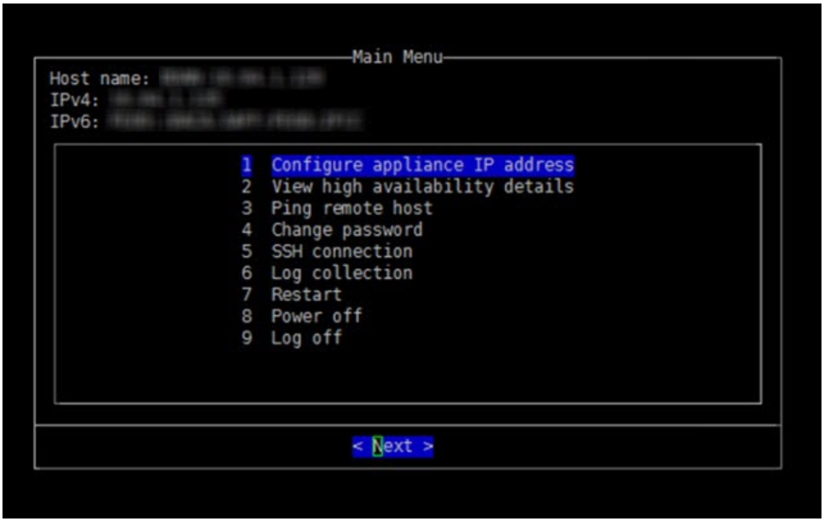
Procedure

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

   - User name: `admin`
   - Password: `Admin1234!`

> **Note**
>
> None of the characters you type appear on the screen.
>
> This password is the same as the password used to log on to the web-based management console. For more information, see *Logon Credentials on page 2-12*.

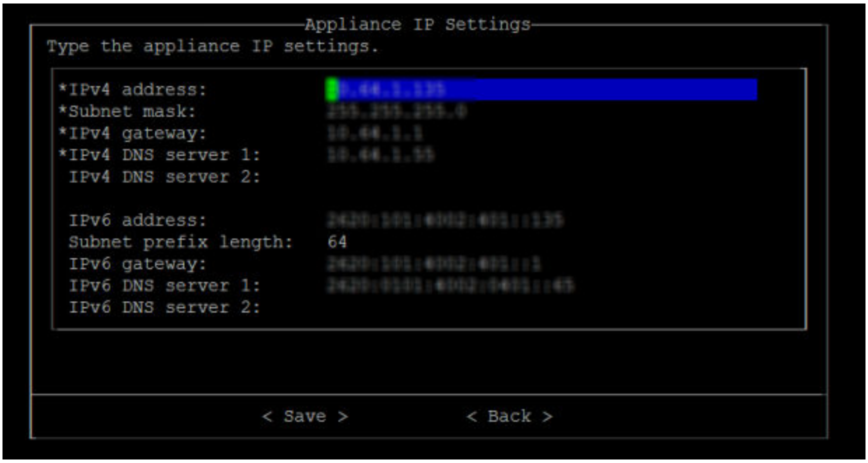
The **Main Menu** screen appears.



```
                         Main Menu
Host name: [redacted]
IPv4: [redacted]
IPv6: [redacted]

              1  Configure appliance IP address
              2  View high availability details
              3  Ping remote host
              4  Change password
              5  SSH connection
              6  Log collection
              7  Restart
              8  Power off
              9  Log off

                         < Next >
```

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

   The **Appliance IP Settings** screen appears.



```
                   Appliance IP Settings
Type the appliance IP settings.

 *IPv4 address:           [redacted]
 *Subnet mask:            [redacted]
 *IPv4 gateway:           [redacted]
 *IPv4 DNS server 1:      [redacted]
  IPv4 DNS server 2:

  IPv6 address:           [redacted]
  Subnet prefix length:   64
  IPv6 gateway:           [redacted]
  IPv6 DNS server 1:      [redacted]
  IPv6 DNS server 2:

              < Save >          < Back >
```

3. Specify the following required settings:

ITEM	GUIDELINES
IPv4 address	• Must be in the same subnet as the virtual IP address. • Must not conflict with the following addresses: • Sandbox network: Configured in **Virtual Analyzer** > **Sandbox Management** > **Network Connection** • Virtual IP address: Configured in **Administration** > **System Settings** > **High Availability** • Virtual Analyzer: `1.1.0.0/27`, `1.1.2.0/24`, `192.0.2.0/24`, `198.18.0.0/15`, `198.51.100.0/24`, and `203.0.113.0/24` • Broadcast: `255.255.255.255` • Multicast: `224.0.0.0` - `239.255.255.255` • Link local: `169.254.1.0` - `169.254.254.255` • Class E: `240.0.0.0` - `255.255.255.255` • Localhost: `127.0.0.1/8` **Note** Changing the IP address changes the management console URL.
Subnet mask	Must use a standard subnet mask format
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.

Viewing High Availability Details on the Preconfiguration Console

Before you begin

The **High Availability** screen looks different depending on the appliance you log on to.

Use the **High Availability** screen to view details about the high availability configuration.

> **Note**
>
> On a passive primary appliance, this screen can be used to detach the appliance from the cluster.

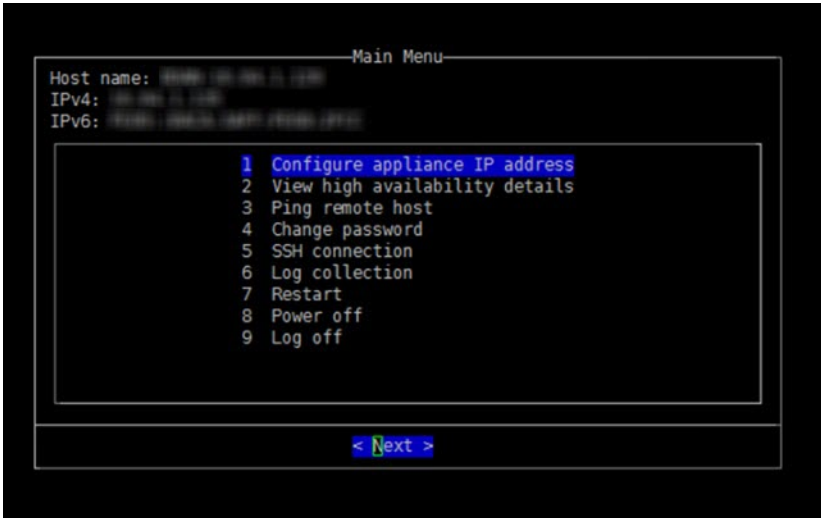
Procedure

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

   - User name: `admin`
   - Password: `Admin1234!`

   > **Note**
   >
   > None of the characters you type appear on the screen.
   >
   > This password is the same as the password used to log on to the web-based management console. For more information, see *Logon Credentials on page 2-12*.

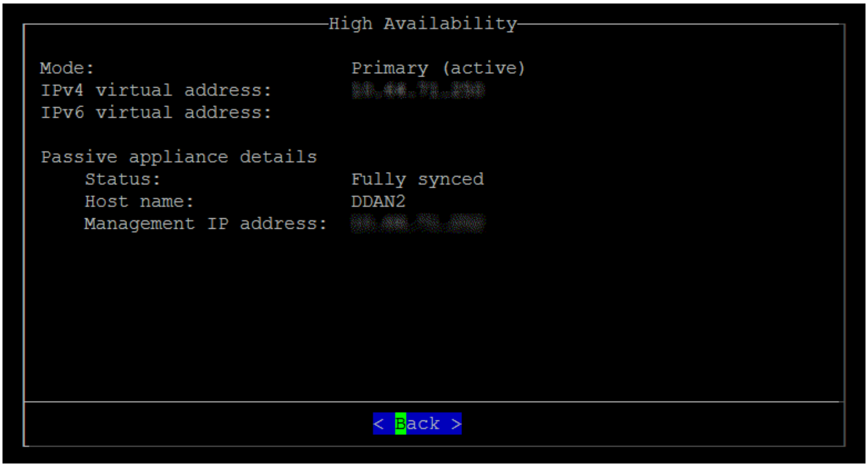
The **Main Menu** screen appears.



```
                         Main Menu
Host name: [redacted]
IPv4: [redacted]
IPv6: [redacted]

              1  Configure appliance IP address
              2  View high availability details
              3  Ping remote host
              4  Change password
              5  SSH connection
              6  Log collection
              7  Restart
              8  Power off
              9  Log off

                        < Next >
```

2. Select **View high availability details** and press ENTER.

The **High Availability** screen appears.



```
                      High Availability

Mode:                        Primary (active)
IPv4 virtual address:        [redacted]
IPv6 virtual address:

Passive appliance details
    Status:                  Fully synced
    Host name:               DDAN2
    Management IP address:   [redacted]

                          < Back >
```

The following table shows the on-screen labels and high availability configuration details.

TABLE 4-1. High Availability Screen

LABEL	DETAIL
Mode	Cluster mode of the appliance.
Status	Sync status of the passive primary appliance.
Host name	Host name of the appliance.
Management IP address	Management IP address of the appliance.
IPv4 virtual address	IPv4 virtual address of the active primary appliance.
IPv6 virtual address	IPv6 virtual address of the active primary appliance.

3. (Optional) On the passive primary appliance, press TAB to navigate to **Detach**, and then press ENTER to detach the passive primary appliance.

   Note

   Detaching the passive primary appliance disables high availability.

4. Press TAB to navigate to **Back**, and then press ENTER.

   The **Main Menu** screen appears.

Chapter 5

Upgrading Deep Discovery Analyzer

This chapter discusses how to upgrade the firmware from previous Deep Discovery Analyzer versions.

Upgrading Firmware on an Appliance

From time to time, Trend Micro releases a new firmware version for a reported known issue or an upgrade that applies to the product. Find available firmware versions at http://downloadcenter.trendmicro.com.

Deep Discovery Analyzer 6.8 supports direct migration of data and configuration settings from the following versions:

- Deep Discovery Analyzer 6.5 Patch 1
- Deep Discovery Analyzer 6.1 Patch 1

You can upgrade the firmware on Deep Discovery Analyzer using one of the following methods:

- The Deep Discovery Analyzer management console
- Plan deployment from Deep Discovery Director. For more information, see the Deep Discovery Director documentation.

Important

If you have multiple Deep Discovery Analyzer appliances deployed and configured to form a cluster, see the migration tasks in *Upgrading Firmware on Appliances in a Cluster on page 5-3*.

Note

Ensure that you have finished all management console tasks before proceeding. The upgrade process may take some time to complete.

Procedure

1. Obtain the firmware image.

    - Download the Deep Discovery Analyzer firmware image from the Trend Micro Download Center at:

      http://downloadcenter.trendmicro.com

- Obtain the firmware package from your Trend Micro reseller or support provider.

2. On the logon page of the management console, select **Enable extended session timeout** and then log on using a valid user name and password.

3. Back up configuration settings. Do the following:

   a. Go to **Administration** > **System Maintenance** and click the **Back Up** tab.

   b. Click **Export**.

4. Go to **Administration** > **Updates**, and then click the **Firmware** tab.

5. Click **Choose File** or **Browse**, and then select the firmware upgrade file.

6. Click **Install**.

   The screen displays the firmware upgrade status.

   > **Important**
   >
   > Do not close or refresh the browser, navigate to another page, perform tasks on the management console, or power off the appliance until updating is complete.
   >
   > Deep Discovery Analyzer will automatically restart after the firmware upgrade is complete.

7. Clear the browser cache before you access the management console.

Upgrading Firmware on Appliances in a Cluster

If you have multiple Deep Discovery Analyzer appliances deployed and configured to form a cluster, follow the procedure for the cluster configuration to upgrade the Deep Discovery Analyzer appliances.

TABLE 5-1. Firmware upgrade procedures for appliances in a cluster

CLUSTER CONFIGURATION	TASKS
High availability cluster	1. Detach the passive primary appliance. 2. Individually upgrade both the active primary appliance and the passive primary appliance. For more information, see *Upgrading Firmware on an Appliance on page 5-2*. 3. Add the passive primary appliance to the cluster again.
Load-balancing cluster	Individually upgrade all Deep Discovery Analyzer appliances.
High availability cluster with load balancing	1. Detach the passive primary appliance. 2. Individually upgrade both the active primary appliance and the passive primary appliance. For more information, see *Upgrading Firmware on an Appliance on page 5-2*. 3. Add the passive primary appliance to the cluster again. 4. Individually upgrade all secondary appliances. For more information, see *Upgrading Firmware on an Appliance on page 5-2*.

Chapter 6

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 6-2*
- *Contacting Trend Micro on page 6-3*
- *Sending Suspicious Content to Trend Micro on page 6-4*
- *Other Resources on page 6-5*

Troubleshooting Resources

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

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 from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

   Tip

   To submit a support case online, visit the following URL:

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

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

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, 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://about-threats.trendmicro.com/us/threatencyclopedia#malware 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 or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
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 connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- 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.

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/1112106.aspx

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.

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.

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.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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

Appendix A

Getting Started

This chapter describes how to get started with Deep Discovery Analyzer and configure initial settings.

The Management Console

Deep Discovery Analyzer provides a built-in management console for configuring and managing the product.

Open the management console from any computer on the management network with the following resources:

- Microsoft Internet Explorer™ 9, 10, or 11
- Microsoft Edge™
- Google Chrome™
- Mozilla Firefox™

To log on, open a browser window and type the following URL:

`https://<Appliance IP Address>/pages/login.php`

This opens the logon screen, which shows the following options:

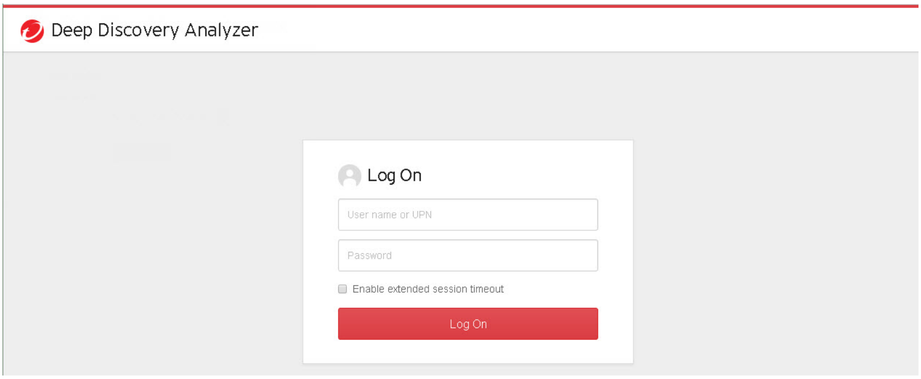


TABLE A-1. Management Console Logon Options

OPTION	DETAILS
User name	Type the logon credentials (user name and password) for the management console. Use the default administrator logon credentials when logging on for the first time: • User name: `admin` • Password: `Admin1234!` Trend Micro recommends changing the password after logging on to the management console for the first time. Configure user accounts to allow other users to access the management console without using the administrator account. For details, see *Accounts Tab on page A-3*.
Password	
Enable extended session timeout	Select this option to apply the extended session timeout for your logon session. The default session timeout is 10 minutes. To change the session timeout settings, navigate to **Administration** > **System Settings** and click the **Session Timeout** tab.
Log On	Click **Log On** to log on to the management console.

Accounts Tab

Use the **Accounts** tab to create and manage user accounts.

Procedure

1. Go to **Administration** > **Accounts / Contacts**.

2. Use the following options to manage user accounts:

   - To add a new user account, click **Add** .

The **Add Account** window opens. For details, see *Add / Edit Account on page A-5*.

- To delete an account, select one or more user accounts and click **Delete**.

Important

- You cannot delete the default Deep Discovery Analyzer administrator account.
- You cannot delete the logged-on account.

- To manually unlock an account, select a user account and click **Unlock**.

  Deep Discovery Analyzer includes a security feature that locks an account in case the user typed an incorrect password five times in a row. This feature cannot be disabled. Locked accounts automatically unlock after ten minutes. The administrator can manually unlock accounts that have been locked.

  Only one user account can be unlocked at a time.

3. To make changes to an existing account, click the user name of the account.

   The **Edit Account** window opens. For details, see *Add / Edit Account on page A-5*.

4. If there are many entries in the table, use the following options to manage the user accounts list:

   - Select an account type from the **Type** drop down to show only the accounts for a specific type.
   - Click the **Name** column to sort names alphabetically.
   - Type a few characters in the **Search** text box to narrow down the entries. As you type, the entries that match the characters you typed are displayed. Deep Discovery Analyzer searches all cells in the current page for matches.
   - The panel at the bottom of the screen shows the total number of user accounts. If all user accounts cannot be displayed at the same time, use the pagination controls to view the accounts that are hidden from view.

Add / Edit Account

The **Add Account** and **Edit Account** screens share similar options.

Procedure

1. Go to **Administration** > **Accounts / Contacts**, and then go to the **Account** tab.

    - Click **Add** to open the **Add Account** screen.
    - Click the user name of an existing user account to open the **Edit Account** screen.

2. To add a local account, select **Local user** as the account **Type**, and provide the following details.

    - **Name**: Name of the account owner.
    - **User name**: User name supports a maximum of 40 characters.
    - **Password**: Type a password that contains at least 8 characters and includes uppercase letters, lowercase letters, numbers, and special characters.

    > Note
    >
    > - To increase password complexity requirements, configure the global password policy in **Administration** > **System Settings** > **Password Policy** tab. The password policy is displayed in the window and must be satisfied before you can add a user account.
    > - When a user exceeds the number of retries allowed while entering incorrect passwords, Deep Discovery Analyzer sets the user account to inactive (locked). You can unlock the account in the **Accounts** screen.

    - **Confirm password**: Type the password again.
    - (Optional) **Description**: Description supports a maximum of 40 characters.

3. To add an Active Directory user, select **Active Directory user** as the account **Type**, and provide the following details.

    - **User name or group**: Specify the User Principal Name (UPN) or user group name.

> **Note**
>
> To quickly locate a specific user name or group, type a few characters in the text box and click **Search**.

- (Optional) **Description**: Description supports a maximum of 40 characters.

4. Select the role and associated permissions of the user account.

    - **Administrator**: Users have full access to submitted objects, analysis results, and product settings
    - **Investigator**: Users have read-only access to submitted objects, analysis results, and product settings, but can submit objects and download the investigation package, including submitted objects
    - **Operator**: Users have read-only access to submitted objects, analysis results, and product settings

5. (Optional) Select **Add to contacts** to add the user account to the **Contacts** list, and provide the following details:

    > **Note**
    >
    > Contacts receive email alert notifications by default.

    - **Email address**
    - (Optional) **Phone number**

6. Click **Save**.

Getting Started Tasks

Procedure

1. Activate the product license using a valid Activation Code. For details, see *License on page A-8*.

2. Specify the Deep Discovery Analyzer host name and IP address. For details, see *Network Tab on page A-10*.

3. Configure proxy settings if Deep Discovery Analyzer connects to the management network or Internet through a proxy server. For details, see *Proxy Tab on page A-12*.

4. Configure date and time settings to ensure that Deep Discovery Analyzer features operate as intended. For details, see *Time Tab on page A-14*.

5. Configure SMTP settings to enable sending of notifications through email. For details, see *SMTP Tab on page A-16*.

6. Import sandbox instances to Virtual Analyzer. For details, see *Importing an Image on page A-17*.

7. Configure Virtual Analyzer network settings to enable sandbox instances to connect to external destinations. For details, see *Enabling External Connections on page A-19*.

8. (Optional) Deploy and configure additional Deep Discovery Analyzer appliances for use in a high availability or load-balancing cluster. For details, see *Cluster Tab on page A-21*.

9. Configure supported Trend Micro products for integration with Deep Discovery Analyzer.

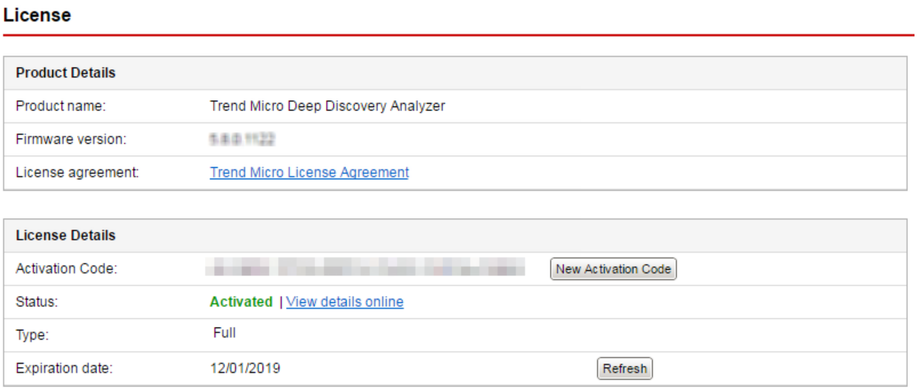
   For details, see the Deep Discovery Analyzer Administrator's Guide.

10. Adjust Virtual Analyzer resource allocation between all sources by assigning weight and timeout values to all sources that submit objects to Deep Discovery Analyzer for analysis.

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

License

Use the **License** screen, in **Administration** > **License**, to view, activate, and renew the Deep Discovery Analyzer license.



License

Product Details	
Product name:	Trend Micro Deep Discovery Analyzer
Firmware version:	[redacted]
License agreement:	Trend Micro License Agreement

License Details	
Activation Code:	[redacted]
Status:	Activated | View details online
Type:	Full
Expiration date:	12/01/2019

The Deep Discovery Analyzer license includes product updates (including ActiveUpdate) and basic technical support ("Maintenance") for one (1) year from the date of purchase. The license allows you to upload threat samples for analysis, and to access Trend Micro Threat Connect from Virtual Analyzer. In addition, the license allows you to send samples to the Trend Micro cloud sandboxes for analysis.

After the first year, Maintenance must be renewed on an annual basis at the current Trend Micro rate.

A Maintenance Agreement is a contract between your organization and Trend Micro. It establishes your right to receive technical support and product updates in return for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

The Maintenance Agreement has an expiration date. Your License Agreement does not. If the Maintenance Agreement expires, you will no longer be entitled to receive technical support from Trend Micro or access Trend Micro Threat Connect.

Typically, 90 days before the Maintenance Agreement expires, you will start to receive email notifications, alerting you of the pending discontinuation. You can update your

Maintenance Agreement by purchasing renewal maintenance from your Reseller, Trend Micro sales, or on the Trend Micro Customer Licensing Portal at:

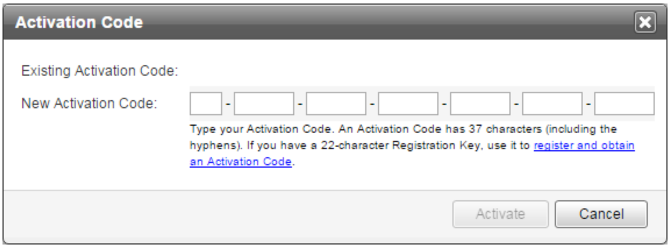
https://clp.trendmicro.com/fullregistration

The **License** screen includes the following information and options.

TABLE A-2. Product Details

FIELD	DETAILS
Product name	Displays the name of the product.
Firmware version	Displays the full build number of the product.
License agreement	Displays a link to the **Trend Micro License Agreement**. Click the link to view or print the license agreement.

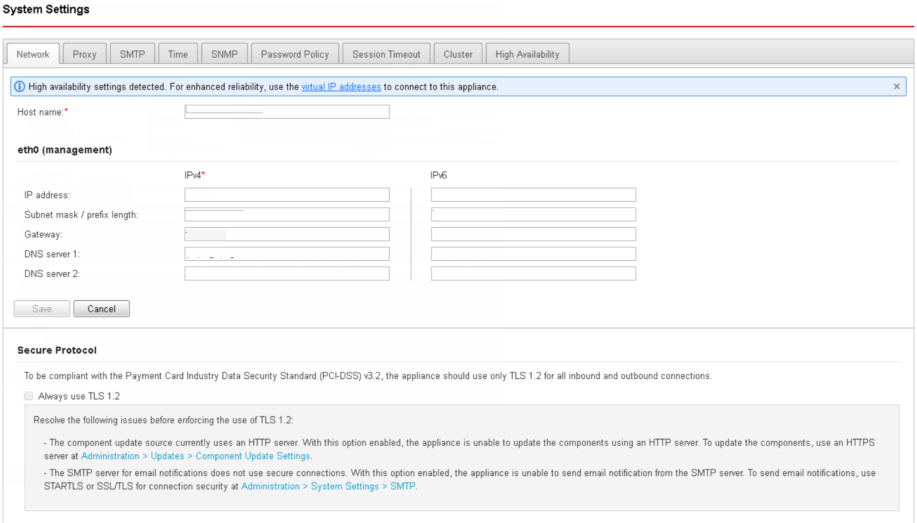
TABLE A-3. License Details

FIELD	DETAILS
Activation Code	View the Activation Code in this section. If your license has expired, obtain a new Activation Code from Trend Micro. To renew the license, click **New Activation Code**, and type the new Activation Code.  Activation Code Existing Activation Code: New Activation Code: Activate Cancel Type your Activation Code. An Activation Code has 37 characters (including the hyphens). If you have a 22-character Registration Key, use it to register and obtain an Activation Code. The **License** screen reappears displaying the number of days left before the product expires.

Field	Details
Status	Displays either **Activated**, **Not Activated**, **Grace Period**, **Expired**, or **Evaluation Expired**. Click **View details online** to view detailed license information from the Trend Micro website. If the status changes (for example, after you renewed the license) but the correct status is not indicated in the screen, click **Refresh**.
Type	• Full: Provides access to all product features • Evaluation: Provides access to all product features
Expiration date	View the expiration date of the license. Renew the license before it expires.

Network Tab

Use this screen to configure the host name, the IPv4 and IPv6 addresses of the Deep Discovery Analyzer appliance, and other network settings (including TLS 1.2 enforcement).



High availability settings detected. For enhanced reliability, use the virtual IP addresses to connect to this appliance.

To be compliant with the Payment Card Industry Data Security Standard (PCI-DSS) v3.2, the appliance should use only TLS 1.2 for all inbound and outbound connections.

□ Always use TLS 1.2

Resolve the following issues before enforcing the use of TLS 1.2:

- The component update source currently uses an HTTP server. With this option enabled, the appliance is unable to update the components using an HTTP server. To update the components, use an HTTPS server at Administration > Updates > Component Update Settings.

- The SMTP server for email notifications does not use secure connections. With this option enabled, the appliance is unable to send email notification from the SMTP server. To send email notifications, use STARTLS or SSL/TLS for connection security at Administration > System Settings > SMTP.

An IPv4 address is required and the default is `192.168.252.2`. Modify the IPv4 address immediately after completing all deployment tasks.

Note

You can also use the **Preconfiguration Console** to modify the network settings.

For details, see the *Configuring Network Addresses on the Preconfiguration Console on page 4-5*.

Deep Discovery Analyzer uses the specified IP addresses to connect to the Internet when accessing Trend Micro hosted services, including the Smart Protection Network, the ActiveUpdate server, and Threat Connect. The IP addresses also determine the URLs used to access the management console.

You can select **Enable TLS 1.2** to enhance data security for inbound and outbound connections on Deep Discovery Analyzer.

Note

To be compliant with the Payment Card Industry Data Security Standard (PCI-DSS) v3.2, the appliance should use only TLS 1.2 for all inbound and outbound connections.

Ensure that the integrated products and services are using the latest version that supports TLS 1.2. For details, see the Deep Discovery Analyzer Adminstrator's Guide.

Verify that the following products/services are configured to use TLS 1.2.

- The ActiveUpdate server source at **Administration** > **Updates** > **Component Update Settings** must use HTTPS.
- The ICAP settings at **Administration** > **Integrated Products/Services** > **ICAP** must use ICAP over SSL.
- The syslog servers at **Administration** > **Integrated Products/Services** > **Syslog** must use SSL.
- The SMTP server at **Administration** > **System Settings** > **SMTP** must use SSL/TLS or STARTTLS.

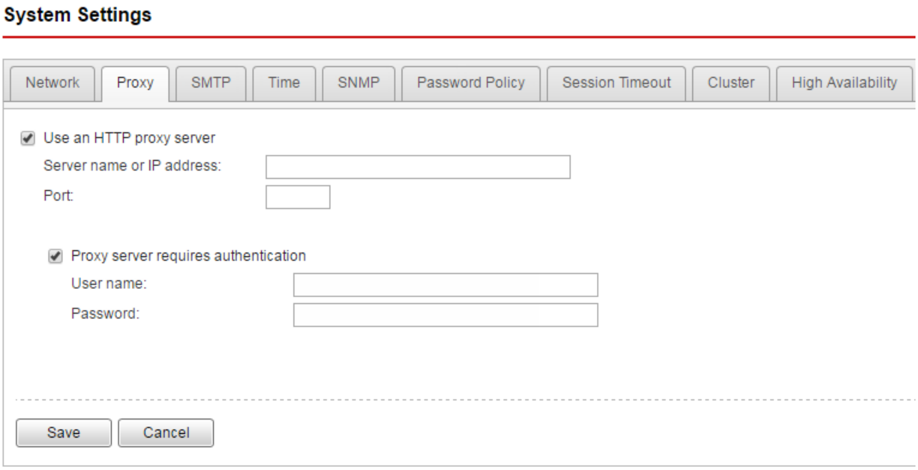
The following table lists configuration limitations.

Table A-4. Configuration Limitations

Field	Limitation
Host name	Cannot be modified when using high availability
IPv4 address	• Must differ from IPv4 virtual address • Must be in the same network segment as IPv4 virtual address
IPv6 address	• Must differ from IPv6 virtual address • Must be in the same network segment as IPv6 virtual address • Cannot be deleted if IPv6 virtual address has been configured • Cannot be added or deleted when using high availability

Proxy Tab

Specify proxy settings if Deep Discovery Analyzer connects to the Internet or management network through a proxy server.



☑ Use an HTTP proxy server

Server name or IP address:

Port:

☑ Proxy server requires authentication

User name:

Password:

Configure the following settings.

Table A-5. Proxy Tab Tasks

Task	Steps
Use an HTTP proxy server	Select this option to enable proxy settings.
Server name or IP address	Type the proxy server host name or IPv4 address, or IPv6 address. The management console does not support host names with double-byte encoded characters. If the host name includes such characters, type its IP address instead.
Port	Type the port number that Deep Discovery Analyzer uses to connect to the proxy server.
Proxy server requires authentication	Select this option if the connection to the proxy server requires authentication. Deep Discovery Analyzer supports the following authentication methods: • No authentication • Basic authentication • Digest authentication • NTLMv1 authentication
User name	Type the user name used for authentication. **Note** This option is only available if **Proxy server requires authentication** is enabled.
Password	Type the password used for authentication. **Note** This option is only available if **Proxy server requires authentication** is enabled.

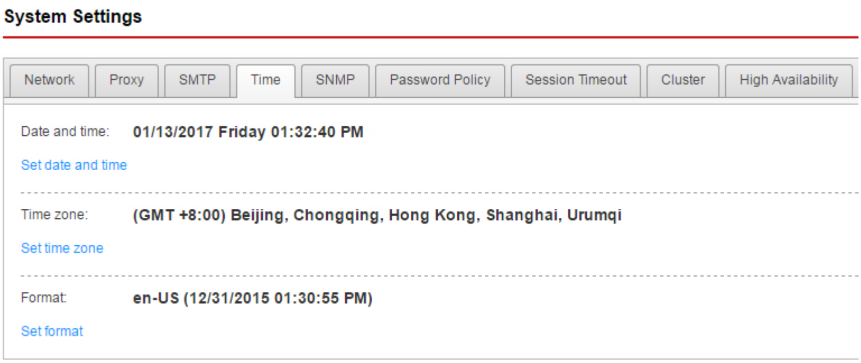
Time Tab

Configure date and time settings immediately after installation.

Procedure

1. Go to **Administration** > **System Settings** and click the **Time** tab.

   The **Time** screen appears.



System Settings

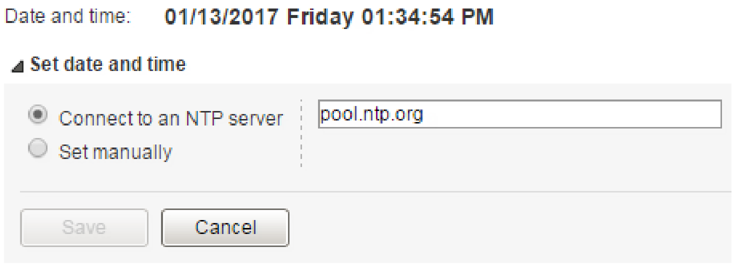
Date and time: 01/13/2017 Friday 01:32:40 PM

Time zone: (GMT +8:00) Beijing, Chongqing, Hong Kong, Shanghai, Urumqi

Format: en-US (12/31/2015 01:30:55 PM)

2. Click **Set date and time**.

   The settings panel appears.



Date and time: 01/13/2017 Friday 01:34:54 PM

◢ Set date and time

● Connect to an NTP server: pool.ntp.org

○ Set manually

3. Select one of the following methods and configure the applicable settings.

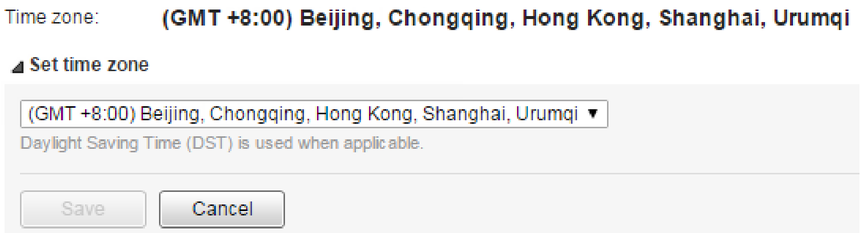
   - Select **Connect to an NTP server** and type the host name, IPv4 address, or IPv6 address of the NTP server.

- Select **Set manually** and configure the time.

4. Click **Save**.

5. Click **Set time zone**.

   The settings panel appears.



Time zone: **(GMT +8:00) Beijing, Chongqing, Hong Kong, Shanghai, Urumqi**

◢ **Set time zone**

(GMT +8:00) Beijing, Chongqing, Hong Kong, Shanghai, Urumqi ▼

Daylight Saving Time (DST) is used when applicable.

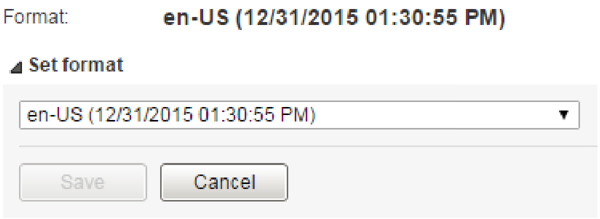
6. Select the applicable time zone.

> **Note**
>
> Daylight Saving Time (DST) is used when applicable.

7. Click **Save**.

8. Click **Set format**.

   The settings panel appears.



Format: **en-US (12/31/2015 01:30:55 PM)**

◢ **Set format**

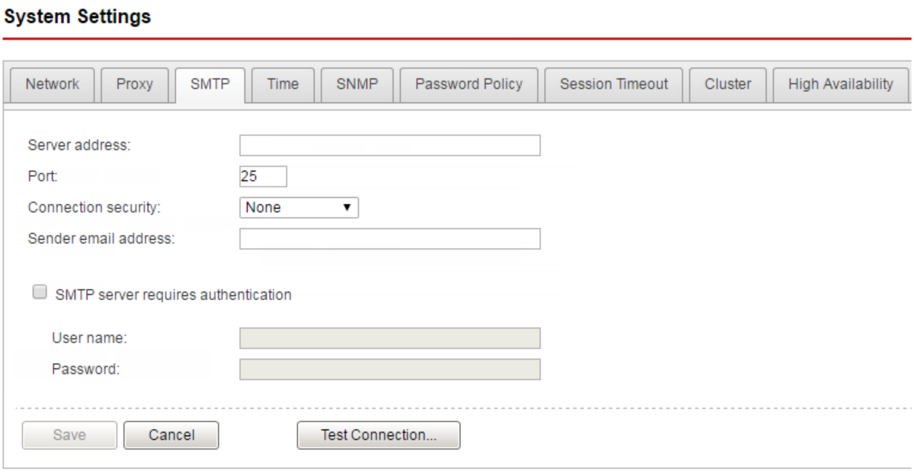
en-US (12/31/2015 01:30:55 PM) ▼

9. Select the preferred date and time format.

10. Click **Save**.

SMTP Tab

Deep Discovery Analyzer uses SMTP settings when sending notifications through email.



Port: 25

Connection security: None

□ SMTP server requires authentication

Procedure

1. Go to **Administration** > **System Settings** and click the **SMTP** tab.

2. Specify the following details:

Table A-6. SMTP Tab Tasks

Field	Steps
Server address	Type the SMTP server host name, IPv4 address, or IPv6 address. The management console does not support host names with double-byte encoded characters. If the host name includes such characters, type its IP address instead.
Port	Type the port number used by the SMTP server.

FIELD	STEPS
Connection security	Specify the type of security used for the connection. Available values are: None, STARTTLS, SSL/TLS.
Sender email address	Type the email address of the sender. The default value is `notifications@ddan.local`.
SMTP server requires authentication	If the server requires authentication, select **SMTP server requires authentication** and specify a user name and password. **WARNING!** Ensure that the user name and password to be specified is valid for the SMTP server. Connections made using an incorrect user name and password may cause some SMTP servers to reject all network request originating from the Deep Discovery Analyzer server.

3. (Optional) To test the connection to the external SMTP server, do the following:

   a. Click **Test Connection**.

   b. Type the recipient email address.

   c. Click **OK**.

   Note

   Deep Discovery Analyzer does not send a test email message to the recipient.

4. Click **Save**.

Importing an Image

You can import up to three images. The hardware specifications of your product determine the number of instances that you can deploy per image.

On Deep Discovery Analyzer 1000 appliances, Virtual Analyzer supports OVA files up to 20GB in size.

On Deep Discovery Analyzer 1100 and 1200 appliances, Virtual Analyzer supports OVA files up to 30GB in size.

Important

Virtual Analyzer stops analysis and keeps all samples in the queue whenever an image is added or deleted, or when instances are modified.

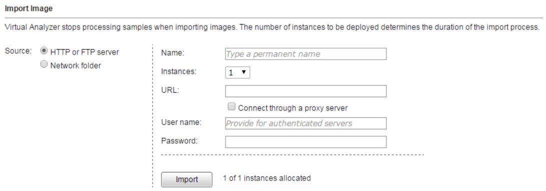
Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Images** tab.

   The **Images** screen appears.

2. Click **Import**.

   The **Import Image** screen appears.



Import Image

Virtual Analyzer stops processing samples when importing images. The number of instances to be deployed determines the duration of the import process.

Source: ● HTTP or FTP server ○ Network folder

Name:	*Type a permanent name*
Instances:	1 ▼
URL:	
	□ Connect through a proxy server
User name:	*Provide for authenticated servers*
Password:	

1 of 1 instances allocated

3. Select an image source and configure the applicable settings.

   a. Type a permanent image name with a maximum of 50 characters.

   b. Choose the number of instances to allocate for the image.

   Note

   Trend Micro recommends distributing the number of instances evenly across all deployed images. Submitted objects must pass through all images before analysis results are generated.

c. Type the URL or network share path of the OVA file.

d. (Optional) Select **Connect through a proxy sever**.

e. (Optional) Type the logon credentials if authentication is required.

4. Click **Import**.

   Virtual Analyzer validates the OVA files before starting the import process.

   Note

   - If you selected **HTTP or FTP server**, Deep Discovery Analyzer downloads the images first before importing into Virtual Analyzer. The process can only be canceled before the download completes.
   - Deep Discovery Analyzer supports connection to a source HTTP server that complies with HTTP/1.0 or later.

Enabling External Connections

Sample analysis is paused and settings are disabled whenever Virtual Analyzer is being configured.

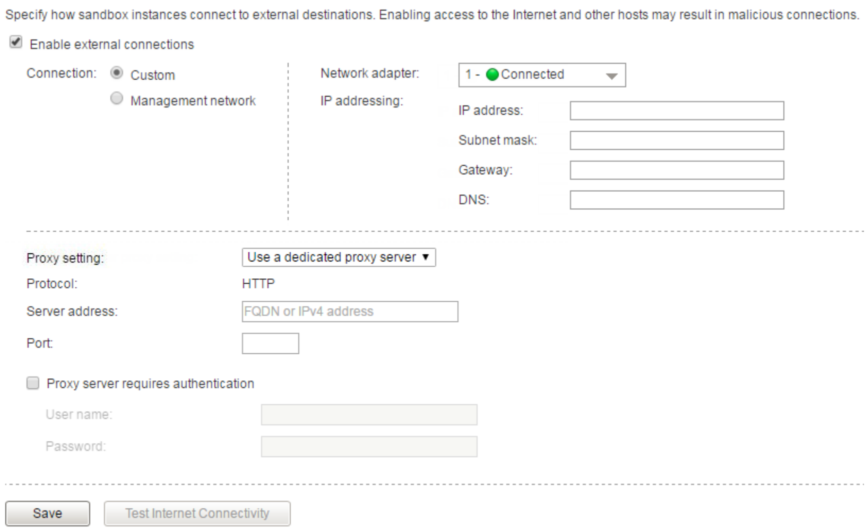
Procedure

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Network Connection** tab.

   The **Network Connection** screen appears.

2. Select **Enable external connections**.

The settings panel appears.



Specify how sandbox instances connect to external destinations. Enabling access to the Internet and other hosts may result in malicious connections.

☑ Enable external connections

Connection: ● Custom ○ Management network

Network adapter: 1 - ● Connected

IP addressing:

IP address:

Subnet mask:

Gateway:

DNS:

Proxy setting: Use a dedicated proxy server ▾

Protocol: HTTP

Server address: FQDN or IPv4 address

Port:

□ Proxy server requires authentication

User name:

Password:

3. Select the type of connection to be used by sandbox instances.

- Custom: Any user-defined network

Important

Trend Micro recommends using an environment isolated from the management network.

- Management network: Default organization Intranet

WARNING!

Enabling connections to the management network may result in malware propagation and other malicious activity in the network.

4. If you selected **Custom**, specify the following:

- Network adapter: Select an adapter with a linked state.

- IP address: Type an IPv4 address.
- Subnet mask
- Gateway
- DNS

5. If the sandbox requires a proxy server for network connection, select **Use a dedicated proxy server**, and specify the following.

   - Server address
   - Port
   - User name: This option is only available if **Proxy server requires authentication** is enabled.
   - Password: This option is only available if **Proxy server requires authentication** is enabled.

6. Click **Save**.

Cluster Tab

Multiple standalone Deep Discovery Analyzer appliances can be deployed and configured to form a cluster that provides fault tolerance, improved performance, or a combination thereof.

Depending on your requirements and the number of Deep Discovery Analyzer appliances available, you may deploy the following cluster configurations:

TABLE A-7. Cluster Configurations

CLUSTER CONFIGURATION	DESCRIPTION
High availability cluster	In a high availability cluster, one appliance acts as the active primary appliance, and one acts as the passive primary appliance. The passive primary appliance automatically takes over as the new active primary appliance if the active primary appliance encounters an error and is unable to recover.
Load-balancing cluster	In a load-balancing cluster, one appliance acts as the active primary appliance, and any additional appliances act as secondary appliances. The secondary appliances process submissions allocated by the active primary appliance for performance improvement.
High availability cluster with load balancing	In a high availability cluster with load balancing, one appliance acts as the active primary appliance, one acts as the passive primary appliance, and any additional appliances act as secondary appliances. The passive primary appliance takes over as the active primary appliance if the active primary appliance encounters an error and is unable to recover. The secondary appliances process submissions allocated by the active primary appliance for performance improvement.

The following table lists the available configuration modes and associated appliance behavior.

TABLE A-8. Cluster Configuration Modes

CONFIGURATION MODE	DESCRIPTION
Primary (Active)	• Management console is fully accessible • Retains all configuration settings

Configuration Mode	Description
Primary (Passive)	• Management console is unavailable • Automatically configured based on the settings of the active primary appliance • On standby • Takes over as the active primary appliance if the active primary appliance encounters an error and is unable to recover • Does not process submissions

Configuration Mode	Description
Secondary	- Automatically configured based on the settings of the active primary appliance - Identifies the active primary appliance using its IP address or virtual IP address - Processes submissions allocated by the active primary appliance for performance improvement - Management console only shows screens with configurable settings: - **Virtual Analyzer** > **Sandbox Management** > **Network Connection** - **Virtual Analyzer** > **Sandbox Management** > **Sandbox for macOS** - **Administration** > **Updates** > **Hotfixes / Patches** - **Administration** > **Updates** > **Firmware** - **Administration** > **System Settings** > **Network** - **Administration** > **System Settings** > **Cluster** - **Administration** > **Accounts / Contacts** > **Accounts** - **Administration** > **Accounts / Contacts** > **Contacts** - **Administration** > **System Logs** - **Administration** > **System Maintenance** > **Network Services Diagnostics** - **Administration** > **System Maintenance** > **Power Off / Restart** - **Administration** > **System Maintenance** > **Debug** - **Administration** > **License**

Nodes List

The **Nodes** list is displayed on the active primary appliance.

The Nodes list contains the following information:

TABLE A-9. Nodes List Columns

COLUMN	DESCRIPTION
Status	Connection status of the appliance. Mouseover a status icon to view details.
Mode	Cluster mode of the appliance.
Management IP Address	Management IP address of the appliance.
Host Name	Host name of the appliance.
Last Connected	Date and time that the appliance last connected to the active primary appliance. **Note** No data (indicated by a dash) if the appliance is a passive primary appliance.

Column	Description
Details	Additional details about the operational status of the appliance. • For standalone appliance: ◦ **Standalone appliance**: The appliance is a standalone appliance. • For passive primary appliance: ◦ **Fully synced**: The passive primary appliance is fully synced to the active primary appliance. ◦ **Syncing n%**: The passive primary appliance is syncing settings from the active primary appliance. ◦ **Sync error**: The passive primary appliance is unable to connect to the active primary appliance. Verify that the appliances are directly connected using eth3, and that eth3 is not used for sandbox analysis. **Tip** This field also displays the connection latency and throughput information. • For secondary appliances: ◦ **Inconsistent component version**: One or more components have different versions on the active primary appliance and secondary appliance. Use the same component versions on all appliances. ◦ **Not connected**: The active primary appliance did not receive a heartbeat from the secondary appliance within the last 10 seconds. Verify that the secondary appliance is powered on and able to connect to the active primary appliance through the network. ◦ **Invalid API key**: The secondary appliance is configured with an invalid API key. Verify the **Active primary API key** on the secondary appliance. ◦ **Incompatible software version**: The firmware, hotfix, and patch versions on the active primary appliance and secondary appliance are different. Use the same firmware, hotfix, and patch version on all appliances. ◦ **Unexpected error**: An unexpected error has occurred. If the issue persists, contact your support provider.

Column	Description
Action	Actions that can be executed depending on the appliance mode and status. • For active primary appliance: • **Swap**: Swap the roles of the primary appliances. Sets the current passive primary appliance to primary mode (active) and the current active primary appliance to primary mode (passive). Appears when the passive primary appliance has synced all settings from the active primary appliance. For details, see *Swapping the Active Primary Appliance and the Passive Primary Appliance on page A-30* • For passive primary appliance: • **Detach**: Detach the passive primary appliance. Disables high availability and allows the passive primary appliance to be used as a standalone appliance. Appears when the passive primary appliance has synced all settings from the active primary appliance. For details, see *Detaching the Passive Primary Appliance from the Cluster on page A-30* • **Remove**: Remove inaccessible passive primary appliance. Disables high availability. Appears when the active primary appliance is unable to reach the passive primary appliance through eth3. For details, see *Removing the Passive Primary Appliance from the Cluster on page A-30* • For secondary appliances: • **Remove**: Remove inaccessible secondary appliance. Affects object processing capacity. Secondary appliances attempt to connect to the active primary appliance every 10 seconds. Appears when the active primary appliance does not receive a heartbeat from the secondary appliance within one minute. For details, see *Removing a Secondary Appliance from the Cluster on page A-33*

Click **Refresh** to refresh the information in the **Nodes** list.

Adding a Passive Primary Appliance to the Cluster

The following table lists requirements that need to be fulfilled by both active primary appliance and passive primary appliance before the passive primary appliance can be added to the cluster.

TABLE A-10. High Availability Clustering Requirements

REQUIREMENT	DESCRIPTION
Hardware model	Must be same hardware model (1000, 1100 or 1200)
Physical connection	Must be directly connected to each other using eth3
Firmware, hotfix, and patch version	Must be the same
Host name	Must be different
IP addresses	Must be symmetrical: • If only IPv4 address is configured on active primary appliance, passive primary appliance cannot configure both IPv4 address and IPv6 address. • If IPv4 address and IPv6 address are configured on active primary appliance, passive primary appliance cannot only configure IPv4 address.
Network segment	Must be in the same network segment
Virtual IP address	Must be configured on the active primary appliance

In a high availability cluster, one appliance acts as the active primary appliance, and one acts as the passive primary appliance. The passive primary appliance automatically takes over as the new active primary appliance if the active primary appliance encounters an error and is unable to recover.

Note

- If your network has Trend Micro Apex Central, only register the active primary appliance to Apex Central.
- When using high availability, use the virtual IP address to register.

Procedure

1. Perform the installation and deployment tasks as described in *Installing the Appliance on page 3-1*.

2. Configure the passive primary appliance.

   a. On the management console of the passive primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.

   b. Select **Primary mode (passive)**.

   c. Type the IPv4 address or IPv6 address of the active primary appliance in **Active primary IP address**.

   d. Click **Test Connection**.

   e. Click **Save**.

   You will be redirected to the appliance standby screen.

- The passive primary appliance stops processing objects if it was previously doing so.

- The passive primary appliance will sync all settings from the active primary appliance. The total time to complete syncing depends on the appliance model.

> **Important**
>
> While the appliance is syncing, it cannot:
>
> - Take over as active primary appliance
> - Switch to another mode

- The management console of the passive primary appliance cannot be accessed. Manage the appliance and monitor the sync status from the management console of the active primary appliance.

Swapping the Active Primary Appliance and the Passive Primary Appliance

Swapping the primary appliances sets the current passive primary appliance to primary mode (active) and the current active primary appliance to primary mode (passive).

Procedure

1. On the management console of the active primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.

2. Click **Swap** to swap the primary appliances.

Detaching the Passive Primary Appliance from the Cluster

Detaching the passive primary appliance disables high availability and allows the appliance to be used as a standalone appliance. After a passive primary appliance is detached, it no longer appears in the nodes list.

Detach the passive primary appliance to update or upgrade the product.

Important

Detaching the passive primary appliance does not reset the appliance settings. Trend Micro recommends reinstalling the appliance if you want to use it as a standalone appliance.

Procedure

1. On the management console of the active primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.

2. Click **Detach** to detach the passive primary appliance from the cluster.

Removing the Passive Primary Appliance from the Cluster

Removing a disconnected or abnormal passive primary appliance from the cluster reduces the clutter in the nodes list.

Procedure

1. On the management console of the active primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.

2. Wait for **Remove** to appear next to the passive primary appliance in the nodes list.

3. Click **Remove** to remove the passive primary appliance from the cluster.

   Note

   The passive primary appliance automatically rejoins the cluster if it reconnects to the active primary appliance.

Adding a Secondary Appliance to the Cluster

Verify that the secondary appliance has the same firmware, hotfix, and patch version as the active primary appliance.

To view the appliance firmware, hotfix, and patch version, see the *Deep Discovery Analyzer Administrator's Guide*.

Update or upgrade the appliance firmware, hotfix, and patch version as necessary. For details, see the *Deep Discovery Analyzer Administrator's Guide*.

Note

- If your network has Trend Micro Apex Central, only register the active primary appliance to Apex Central.
- When using high availability, use the virtual IP address to register.

Procedure

1. Perform the installation and deployment tasks as described in *Installing the Appliance on page 3-1*.

2. Configure the secondary appliance.

a. On the management console of the secondary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.

b. Select **Secondary mode**.

c. Type the IPv4 address or IPv6 address of the active primary appliance in **Active primary IP address**.

> **Note**
>
> If you are using high availability, type the IPv4 virtual address or IPv6 virtual address.

d. Type the **Active primary API key**.

e. Click **Test Connection**.

> **Tip**
>
> Secondary appliances can test their connection to the active primary appliance at any time. Click **Test Connection** to get detailed information about any connectivity problems.

f. Click **Save**.

3. (Optional) Configure additional settings on the secondary appliance.

a. Configure the sandbox network connection setting.

For details, see *Enabling External Connections on page A-19*.

> **Note**
>
> Trend Micro recommends using the external network connection setting of the active primary appliance.

b. Configure the **Sandbox for macOS** setting.

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

c. Configure the appliance network settings.

For details, see *Network Tab on page A-10*.

d. Add accounts.

For details, see *Accounts Tab on page A-3*.

Note

Secondary appliances automatically deploy sandbox instances based on the sandbox allocation ratio of the active primary appliance. The following table lists a configuration example:

Table A-11. Example Configuration Using Two Images

Appliance Type	Deep Discovery Analyzer Hardware Model	Maximum Number of Instances (Total)	Number of Windows 7 Instances	Number of Windows 8.1 Instances
Primary appliance	1200 or 1100	60	40	20
Secondary appliance	1000	33	22	11

Removing a Secondary Appliance from the Cluster

Removing a disconnected secondary appliance from the cluster reduces the clutter in the nodes list and widgets of the active primary appliance.

Procedure

1. On the management console of the active primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.

2. Wait for **Remove** to appear next to the secondary appliance in the nodes list.

Note

Secondary appliances attempt to connect to the active primary appliance every 10 seconds. If the active primary appliance does not receive a heartbeat within one minute, **Remove** appears next to the secondary appliance in the **Nodes** list.

Secondary appliances automatically rejoin the cluster if they reconnect to the active primary appliance.

3. Click **Remove** to remove the secondary appliance from the cluster.

   The secondary appliance is removed from the nodes list and widgets of the active primary appliance.

Replacing the Active Primary Appliance with a Secondary Appliance

If the active primary appliance is unresponsive or cannot be restored, and no passive primary appliance is deployed, it can be replaced by a secondary appliance from the same cluster.

Tip

Trend Micro recommends deployment of a passive primary appliance for high availability. For details, see *Adding a Passive Primary Appliance to the Cluster on page A-28*.

Important

Submissions do not have a result if they were being analyzed on the active primary appliance when it becomes unresponsive.

Procedure

1. Power off the active primary appliance.
2. Select a secondary appliance from the same cluster and configure it as the new active primary appliance.

a. On the management console of the secondary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.

b. Select **Primary mode (active)**.

c. Click **Save**.

3. Configure the IP address of the new active primary appliance.

For details, see *Network Tab on page A-10*.

Note

Trend Micro recommends using the same IP address as the original active primary appliance. This allows secondary appliances and integrated products to connect without reconfiguration.

4. Verify the settings on the new active primary appliance.

Note

Settings take up to one day to propagate to secondary appliances.

Index

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: APEM68831/191002