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:


Trend Micro, the Trend Micro t-ball logo, Control Manager, Deep Discovery, InterScan, OfficeScan, ScanMail, and Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2017. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM57741/170315

Release Date: March 2017

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
# Table of Contents

## Preface

Preface .................................................................................................................. v  
Documentation .................................................................................................. vi  
Audience ............................................................................................................ vii  
Document Conventions .................................................................................. vii  
Terminology ..................................................................................................... viii  
About Trend Micro ............................................................................................ x

## Chapter 1: Introduction

About Deep Discovery Analyzer ................................................................. 1-2  
What's New ..................................................................................................... 1-2  
Features and Benefits ..................................................................................... 1-5  
  Enable Sandboxing as a Centralized Service .............................................. 1-5  
  Custom Sandboxing .................................................................................... 1-5  
  Broad File Analysis Range ...................................................................... 1-6  
  YARA Rules ............................................................................................ 1-6  
  Document Exploit Detection .................................................................. 1-6  
  Automatic URL Analysis ......................................................................... 1-6  
  Detailed Reporting .................................................................................. 1-6  
  Alert Notifications .................................................................................. 1-6  
  Clustered Deployment ........................................................................... 1-7  
  Trend Micro Integration ........................................................................ 1-7  
  Web Services API and Manual Submission ............................................ 1-7  
  Custom Defense Integration ................................................................ 1-7

## Chapter 2: Preparing to Deploy Deep Discovery Analyzer

Deployment Overview ................................................................................... 2-2  
  Product Specifications .............................................................................. 2-2  
  Deployment Considerations .................................................................. 2-3
Chapter 3: Installing the Appliance

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

Chapter 4: Using the Preconfiguration Console

The Preconfiguration Console ................................................ 4-2
Preconfiguration Console Basic Operations ............................ 4-3
Configuring Network Addresses on the Preconfiguration Console ........................................................................ 4-4
Viewing High Availability Details on the Preconfiguration Console .................................................................. 4-7

Chapter 5: Migration

Migrating from previous versions of Deep Discovery Analyzer ........ 5-2
Clearing the Browser Cache .................................................... 5-4

Chapter 6: Technical Support

Troubleshooting Resources ..................................................... 6-2
Using the Support Portal ........................................................ 6-2
Threat Encyclopedia .............................................................. 6-2
Contacting Trend Micro ......................................................... 6-3
Speeding Up the Support Call ............................................... 6-4
Sending Suspicious Content to Trend Micro ......................... 6-4
Email Reputation Services .................................................... 6-4
File Reputation Services ....................................................... 6-5
Web Reputation Services ...................................................... 6-5
Other Resources ................................................................. 6-5
Download Center ............................................................... 6-5
Appendix A: Getting Started

The Management Console ................................................................. A-2
  Accounts Tab ................................................................................ A-3

Getting Started Tasks ........................................................................ A-7
  License .......................................................................................... A-8
  Network Tab .................................................................................. A-10
  Proxy Tab ...................................................................................... A-12
  Time Tab ....................................................................................... A-13
  SMTP Tab ...................................................................................... A-15
  Importing an Image ....................................................................... A-17
  Enabling External Connections ..................................................... A-19
  Cluster Tab .................................................................................... A-21

Index

Index .................................................................................................... IN-1
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**

<table>
<thead>
<tr>
<th>DOCUMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator’s Guide</td>
<td>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.</td>
</tr>
<tr>
<td>Installation and Deployment Guide</td>
<td>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.</td>
</tr>
<tr>
<td>Syslog Content Mapping Guide</td>
<td>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.</td>
</tr>
<tr>
<td>Quick Start Card</td>
<td>The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Analyzer to your network and on performing the initial configuration.</td>
</tr>
<tr>
<td>Readme</td>
<td>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.</td>
</tr>
</tbody>
</table>
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:


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

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPPER CASE</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Menus and menu commands, command buttons, tabs, and options</td>
</tr>
<tr>
<td><em>Italics</em></td>
<td>References to other documents</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Sample command lines, program code, web URLs, file names, and program output</td>
</tr>
<tr>
<td><strong>Navigation &gt; Path</strong></td>
<td>The navigation path to reach a particular screen</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Configuration notes</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Recommendations or suggestions</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>Information regarding required or default configuration settings and product limitations</td>
</tr>
<tr>
<td><strong>WARNING!</strong></td>
<td>Critical actions and configuration options</td>
</tr>
</tbody>
</table>

Terminology

<table>
<thead>
<tr>
<th>TERMINOLOGY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveUpdate Server</td>
<td>Provides updates for product components, including pattern files. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server.</td>
</tr>
<tr>
<td><strong>TERMINOLOGY</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active primary appliance</td>
<td>Clustered appliance with which all management tasks are performed. Retains all configuration settings and allocates submissions to secondary appliances for performance improvement.</td>
</tr>
<tr>
<td>Administrator</td>
<td>The person managing Deep Discovery Analyzer</td>
</tr>
<tr>
<td>Clustering</td>
<td>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.</td>
</tr>
<tr>
<td>Custom port</td>
<td>A hardware port that connects Deep Discovery Analyzer to an isolated network dedicated to sandbox analysis</td>
</tr>
<tr>
<td>Dashboard</td>
<td>UI screen on which widgets are displayed</td>
</tr>
<tr>
<td>High availability cluster</td>
<td>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.</td>
</tr>
<tr>
<td>Load-balancing cluster</td>
<td>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.</td>
</tr>
<tr>
<td>Management console</td>
<td>A web-based user interface for managing a product.</td>
</tr>
<tr>
<td>Management port</td>
<td>A hardware port that connects to the management network.</td>
</tr>
<tr>
<td>Passive primary appliance</td>
<td>Clustered appliance that is on standby until active primary appliance encounters an error and is unable to recover. Provides high availability.</td>
</tr>
<tr>
<td>Role-based administration</td>
<td>Role-based administration streamlines how administrators configure user accounts and control access to the management console.</td>
</tr>
<tr>
<td><strong>TERMINOLOGY</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sandbox image</td>
<td>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.</td>
</tr>
<tr>
<td>Sandbox instance</td>
<td>A single virtual machine based on a sandbox image.</td>
</tr>
<tr>
<td>Secondary appliance</td>
<td>Clustered appliance that processes submissions allocated by the active primary appliance for performance improvement.</td>
</tr>
<tr>
<td>Standalone appliance</td>
<td>Appliance that is not part of any cluster. Clustered appliances can revert to being standalone appliances by detaching the appliance from its cluster.</td>
</tr>
<tr>
<td>Threat Connect</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual Analyzer</td>
<td>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.</td>
</tr>
<tr>
<td>Widget</td>
<td>A customizable screen to view targeted, selected data sets.</td>
</tr>
<tr>
<td>YARA</td>
<td>YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to your environment.</td>
</tr>
</tbody>
</table>

**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 5.8 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.

It 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>
<thead>
<tr>
<th>FEATURE/ENHANCEMENT</th>
<th>DETAILS</th>
</tr>
</thead>
</table>
| Structured Threat Information eXpression (STIX) support | Deep Discovery Analyzer adds support for Structured Threat Information eXpression (STIX) files to perform the following functions:  
  • Use of user-defined match list for detection  
  • Export via the WebService API for 3rd party integration |
| Enhanced SMTP notification           | Deep Discovery Analyzer improves the SMTP notifications feature by adding the following enhancements:  
  • Option to specify the port of SMTP server rather than server address only  
  • Default email sender notifications@ddan.local  
  • Support for SMTP over SSL/TLS and STARTTLS  
  • Option to test connection to SMTP server |
<table>
<thead>
<tr>
<th>FEATURE/ENHANCEMENT</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug log level settings for</td>
<td>The debug log level settings page enables user to configure debug log level setting for ease in troubleshooting.</td>
</tr>
<tr>
<td>troubleshooting</td>
<td></td>
</tr>
<tr>
<td>Enhanced ActiveUpdate</td>
<td>The enhanced ActiveUpdate includes the following features:</td>
</tr>
<tr>
<td></td>
<td>• Several new ActiveUpdate components</td>
</tr>
<tr>
<td></td>
<td>• Option to rollback ActiveUpdate components</td>
</tr>
<tr>
<td></td>
<td>• Frequency of ActiveUpdate update check increased from every 24 hours to every 15 minutes</td>
</tr>
<tr>
<td>Command line arguments for PE</td>
<td>Deep Discovery Analyzer now provides the option to specify optional command line arguments for PE samples received from integrated products,</td>
</tr>
</tbody>
</table>
### Feature/Enhancement Details

**Improved detection capability**

Deep Discovery Analyzer provides increased protection by improving its detection capabilities. This release supports the following:

- Deployment of sandbox images running Windows 10 Threshold 2 (B1511), Windows Server 2012, and Windows Server 2012 R2 operating systems
- Support Microsoft Office 2016 application for Office file analysis in sandbox images
- New file types (Microsoft Publisher 2016, Microsoft Windows Command Script file, Microsoft Windows Batch file, and Scalable Vector Graphics) for file submission filters
- File SHA-256 and vulnerability information in analysis reports
- Decrypt password-protected PDF and Microsoft Office files using a password list
- Extract files in archive files with multiple compression layers

**Enhanced Submission screen**

The enhanced Submission screen includes the following features:

- Improved Advanced filter to provide more search options
- A separate Unsuccessful tab to display all samples which were not successfully analyzed
- Option to customize which columns appear in the Submission screen

**Inline migration from Deep Discovery Analyzer 5.5 and 5.5 SP1**

Deep Discovery Analyzer provides users with the option of automatically migrating the settings from 5.5 and 5.5 SP1 to 5.8 using the Firmware screen of the management console.

**Enhanced credential management**

Deep Discovery Analyzer uses the same user account and password for the admin account on the management console UI and preconfig screen.
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 Integration on page 1-7
• Web Services API and Manual Submission on page 1-7
• Custom Defense 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 Integration

Deep Discovery Analyzer enables out-of-the-box integration to expand the sandboxing capacity 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.
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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack size</td>
<td>2U 19-inch standard rack</td>
</tr>
<tr>
<td>Availability</td>
<td>Raid 5 configuration</td>
</tr>
<tr>
<td>Storage size</td>
<td>2 TB free storage</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack size</td>
<td>2U 19-inch standard rack</td>
</tr>
<tr>
<td>Availability</td>
<td>Raid 1 configuration</td>
</tr>
</tbody>
</table>
### Feature Specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage size</td>
<td>4 TB free storage</td>
</tr>
</tbody>
</table>
| Connectivity           | • Management port: 1 x 10Base-T/100Base-TX/1000Base-T  
                          | • Custom ports: 3 x 10Base-T/100Base-TX/1000Base-T   |
| Dimensions (Wx Dx H)   | 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                          |

### 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**

<table>
<thead>
<tr>
<th>CLUSTER CONFIGURATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>High availability cluster</td>
<td>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 <em>High Availability Cluster on page 2-4.</em></td>
</tr>
<tr>
<td>Load-balancing cluster</td>
<td>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 <em>Load-Balancing Cluster on page 2-6.</em></td>
</tr>
<tr>
<td>High availability cluster with load balancing</td>
<td>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 <em>High Availability Cluster with Load Balancing on page 2-6.</em></td>
</tr>
</tbody>
</table>

**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**

- 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.
- Network switches can be used if a large physical distance does not permit directly connecting the active primary appliance and the passive primary appliance.
  - The active primary appliance and the passive primary appliance must be in the same network segment when using network switches.
  - Trend Micro recommends not connecting any other devices to the network switches used to connect the active primary appliance and the passive primary appliance.

**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.

![Load-Balancing Cluster Diagram]

**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**

- 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.
- Network switches can be used if a large physical distance does not permit directly connecting the active primary appliance and the passive primary appliance.
  - The active primary appliance and the passive primary appliance must be in the same network segment when using network switches.
  - Trend Micro recommends not connecting any other devices to the network switches used to connect the active primary appliance and the passive primary appliance.

**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 its own set of proxy settings, proxy authentication, and connection restrictions. 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

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep Discovery Analyzer</td>
<td>Obtain from Trend Micro</td>
</tr>
<tr>
<td>Deep Discovery Analyzer</td>
<td>Obtain from Trend Micro</td>
</tr>
<tr>
<td>Activation Code</td>
<td>Obtain from Trend Micro</td>
</tr>
<tr>
<td>Monitor and VGA cable</td>
<td>Connects to the VGA port of the appliance</td>
</tr>
<tr>
<td>USB keyboard</td>
<td>Connects to a USB port of the appliance</td>
</tr>
<tr>
<td>USB mouse</td>
<td>Connects to a USB port of the appliance</td>
</tr>
</tbody>
</table>
| 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      |
Logon Credentials

<table>
<thead>
<tr>
<th><strong>Console</strong></th>
<th><strong>Purpose</strong></th>
<th><strong>Default Credentials</strong></th>
<th><strong>Your Information</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Preconfiguration console</td>
<td>Perform initial configuration tasks. See <em>Configuring Network Addresses on the Preconfiguration Console on page 4-4</em>.</td>
<td>• Deep Discovery Analyzer login (not configurable): admin&lt;br&gt;• Password: Admin1234!</td>
<td>Password:</td>
</tr>
<tr>
<td>Management console</td>
<td>• Configure product settings&lt;br&gt;• View and download reports</td>
<td>• User name (not configurable): admin&lt;br&gt;• Password: Admin1234!</td>
<td>Password:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other user accounts (configured on the management console, in Administration &gt; Accounts / Contacts &gt; Accounts)</td>
<td>User account 1:&lt;br&gt;User name:&lt;br&gt;Password:&lt;br&gt;User account 2:&lt;br&gt;User name:&lt;br&gt;Password:</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>FUNCTION</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>TCP</td>
<td>Outbound</td>
<td>Deep Discovery Analyzer uses this port to send backup data to FTP servers.</td>
</tr>
<tr>
<td>22</td>
<td>TCP</td>
<td>Listening and outbound</td>
<td>Deep Discovery Analyzer uses this port to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Access the preconfiguration console with a computer through SSH</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Send backup data to an SFTP server</td>
</tr>
<tr>
<td>53</td>
<td>TCP/UDP</td>
<td>Outbound</td>
<td>Deep Discovery Analyzer uses this port for DNS resolution.</td>
</tr>
<tr>
<td>67</td>
<td>UDP</td>
<td>Outbound</td>
<td>Deep Discovery Analyzer sends requests to the DHCP server if IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>addresses are assigned dynamically.</td>
</tr>
<tr>
<td>68</td>
<td>UDP</td>
<td>Listening</td>
<td>Deep Discovery Analyzer receives responses from the DHCP server.</td>
</tr>
</tbody>
</table>
### Preparing to Deploy Deep Discovery Analyzer

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Function</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 80   | TCP      | Listening and outbound | Deep Discovery Analyzer connects to other computers and integrated Trend Micro products and hosted services through this port.  
In particular, Deep Discovery Analyzer uses this port to:  
- 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 |
<p>| 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. |</p>
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Function</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>Listening and outbound</td>
<td>Deep Discovery Analyzer uses this port to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Access the management console with a computer through HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Communicate with other Deep Discovery Analyzer appliances in a cluster environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Connect to Trend Micro Threat Connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Communicate with Trend Micro Control Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Connect to Web Reputation Services to query the blocking reason</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Receive files from a computer with Manual Submission Tool</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Receive samples from integrated products</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Send anonymous threat information from Smart Feedback</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Send Suspicious Objects list and analysis information to integrated products</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Update components by connecting to the ActiveUpdate server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Verify the safety of files through the Certified Safe Software Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Communicate with Deep Discovery Director</td>
</tr>
</tbody>
</table>
Deep Discovery Analyzer uses user-defined ports to:
- Send logs to syslog servers
- Connect to proxy servers
- Connect to the Smart Protection Server
- 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 3-3.

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

Setting Up the Hardware

Procedure

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

   Note

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

2. Connect the appliance to a power source.

   Deep Discovery Analyzer includes two 750-watt hot-plug power supply units. One acts as the main power supply and the other as a backup. The corresponding AC power slots are located at the back of the appliance, as shown in the following image.
3. Connect the monitor to the VGA port at the back of the appliance.
4. Connect the keyboard and mouse to the USB ports at the back of the appliance.
5. Connect the Ethernet cables to the management and custom ports.
   • **Management port**: A hardware port that connects 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.

---

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.

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

3. Restart the appliance.

   The **POST** screen appears.

The **Boot Manager** screen appears.

5. Under **Boot Manager Main Menu**, select **One-shot BIOS Boot Menu** and press ENTER.

The **Boot Manager** screen appears.
6. Select **DVD-ROM** and press ENTER.
   The **Deep Discovery Analyzer Appliance Installation** screen appears.

7. 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.
8. Click Accept.
The Select Disk screen appears.

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

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

![Hardware Profile Screen]

11. Click **Continue**.

---

**WARNING!**

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

A confirmation message appears.

![Repartition Disks Confirmation]

12. 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 4-4.
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 used to configure network settings, view high availability details, ping remote hosts, and change the preconfiguration console password.

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

<table>
<thead>
<tr>
<th>TASK</th>
<th>PROCEDURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging on</td>
<td>Type valid logon credentials. The default credentials are:</td>
</tr>
<tr>
<td></td>
<td>• User name: admin</td>
</tr>
<tr>
<td></td>
<td>• Password: Admin1234!</td>
</tr>
<tr>
<td>Configuring network addresses</td>
<td>Specify the appliance IP address, subnet mask, gateway, and DNS. For details, see Configuring Network Addresses on the Preconfiguration Console on page 4-4.</td>
</tr>
</tbody>
</table>
### Using the Preconfiguration Console

<table>
<thead>
<tr>
<th>Task</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing high availability details</td>
<td>View the active and passive appliance host names, IP addresses, and sync status.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>High availability cannot be configured on the preconfiguration console. Use the management console to configure high availability. For details see the <em>High Availability Tab</em> and <em>Cluster Tab</em> topics in the <em>Deep Discovery Analyzer Administrator’s Guide</em>.</td>
</tr>
<tr>
<td>Pinging a remote host</td>
<td>Type a valid IP address or FQDN and click <strong>Ping</strong>.</td>
</tr>
<tr>
<td>Changing the preconfiguration console password</td>
<td>Type the new password twice and click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Enabling and disabling SSH connection</td>
<td>Enabling or disabling the SSH connection.</td>
</tr>
<tr>
<td>Logging off</td>
<td>On the <strong>Main Menu</strong>, click <strong>Log off</strong>.</td>
</tr>
</tbody>
</table>

### 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.
Configuring Network Addresses on the Preconfiguration Console

Procedure

1. Type valid logon credentials. The default credentials are:
   - User name: admin
   - Password: Admin1234!
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 2-11.

The Main Menu screen appears.

2. Select Configure appliance IP address and press ENTER.
The **Appliance IP Settings** screen appears.

3. Specify the following required settings:

<table>
<thead>
<tr>
<th>ITEM</th>
<th>GUIDELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 address</td>
<td>Must be in the same subnet as the virtual IP address. Must not conflict with the following addresses:</td>
</tr>
<tr>
<td></td>
<td>• Sandbox network: Configured in <strong>Virtual Analyzer &gt; Sandbox Management &gt; Network Connection</strong></td>
</tr>
<tr>
<td></td>
<td>• Virtual IP address: Configured in <strong>Administration &gt; System Settings &gt; High Availability</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Virtual Analyzer:</strong> 1.1.0.0 - 1.1.2.255</td>
</tr>
<tr>
<td></td>
<td>• <strong>Broadcast:</strong> 255.255.255.255</td>
</tr>
<tr>
<td></td>
<td>• <strong>Multicast:</strong> 224.0.0.0 - 239.255.255.255</td>
</tr>
<tr>
<td></td>
<td>• <strong>Link local:</strong> 169.254.1.0 - 169.254.254.255</td>
</tr>
<tr>
<td></td>
<td>• <strong>Class E:</strong> 240.0.0.0 - 255.255.255.255</td>
</tr>
<tr>
<td></td>
<td>• <strong>Localhost:</strong> 127.0.0.1/8</td>
</tr>
</tbody>
</table>
### Using the Preconfiguration Console

#### Item Guidelines

<table>
<thead>
<tr>
<th>ITEM</th>
<th>GUIDELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet mask</td>
<td>Must not be any of the following numbers:</td>
</tr>
<tr>
<td></td>
<td>- 111.111.111.111</td>
</tr>
<tr>
<td></td>
<td>- 255.255.255.255</td>
</tr>
<tr>
<td>IPv4 gateway</td>
<td>Must be in the same subnet as the IP address</td>
</tr>
<tr>
<td>IPv4 DNS server 1</td>
<td>Same as IP address</td>
</tr>
<tr>
<td>IPv4 DNS server 2 (Optional)</td>
<td>Same as IP address</td>
</tr>
</tbody>
</table>

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 2-11.

The Main Menu screen appears.

2. Select **View high availability details** and press ENTER.
The **High Availability** screen appears.

![High Availability Screen](image)

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

**TABLE 4-1. High Availability Screen**

<table>
<thead>
<tr>
<th>LABEL</th>
<th>DETAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Cluster mode of the appliance.</td>
</tr>
<tr>
<td>Status</td>
<td>Sync status of the passive primary appliance.</td>
</tr>
<tr>
<td>Host name</td>
<td>Host name of the appliance.</td>
</tr>
<tr>
<td>Management IP address</td>
<td>Management IP address of the appliance.</td>
</tr>
<tr>
<td>IPv4 virtual address</td>
<td>IPv4 virtual address of the active primary appliance.</td>
</tr>
<tr>
<td>IPv6 virtual address</td>
<td>IPv6 virtual address of the active primary appliance.</td>
</tr>
</tbody>
</table>

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

Migration

This chapter discusses how to migrate Deep Discovery Analyzer 5.5 and 5.5 SP1 to 5.8.
Migrating from previous versions of Deep Discovery Analyzer

Deep Discovery Analyzer 5.8 supports direct migration of data and configuration settings from the following versions:

- Deep Discovery Analyzer 5.5
- Deep Discovery Analyzer 5.5 SP1

This procedure outlines the steps for migrating the data and configuration settings.

**Important**

If you have multiple Deep Discovery Analyzer appliances deployed and configured to form a cluster, please perform these tasks:

**TABLE 5-1. Cluster Configurations Upgrade Tasks**

<table>
<thead>
<tr>
<th>Cluster Configuration</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>High availability cluster</td>
<td>1. Detach the passive primary appliance.</td>
</tr>
<tr>
<td></td>
<td>2. Individually upgrade both the active primary appliance and the passive primary appliance by performing the tasks as described in the main task section below.</td>
</tr>
<tr>
<td></td>
<td>3. Add the passive primary appliance to the cluster again.</td>
</tr>
<tr>
<td>Load-balancing cluster</td>
<td>Individually upgrade all Deep Discovery Analyzer appliances.</td>
</tr>
<tr>
<td>High availability cluster with load balancing</td>
<td>1. Detach the passive primary appliance.</td>
</tr>
<tr>
<td></td>
<td>2. Individually upgrade both the active primary appliance and the passive primary appliance by performing the tasks as described in the main task section below.</td>
</tr>
<tr>
<td></td>
<td>3. Add the passive primary appliance to the cluster again.</td>
</tr>
</tbody>
</table>
|                                        | 4. Individually upgrade all secondary appliances by performing the tasks as described in the main task section below.
Procedure

1. On the logon page of the management console, select **Extended** and then log on using a valid user name and password.

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

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

4. Click **Apply**.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

Deep Discovery Analyzer will automatically restart after the upgrade is complete.

5. Clear the browser cache.

For details, see *Clearing the Browser Cache on page 5-4*

What to do next

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>• After migration, the ActiveUpdate schedule still retains the old setting as configured in the previous version. Deep Discovery Analyzer does not update the schedule to the new default setting of 15 minutes.</td>
</tr>
</tbody>
</table>

• After upgrading/migrating to this release, the proxy setting for the Virtual Analyzer is not automatically configured to use the global proxy setting, even if the previous Virtual Analyzer network has been configured to use the management network. The proxy setting for the Virtual Analyzer will be empty by default after upgrade/migration.
Clearing the Browser Cache

Procedure

1. On Chrome™:
   a. Go to Settings.
   b. Click Show advanced settings....
   c. Under Privacy, click Clear browsing data....
   d. Select Cookies and other site and plug-in data and Cached images and files.
   e. Click Clear browsing data.

2. On Internet Explorer®:
   a. Go to Tools > Internet Options > General.
   b. Under Browsing history, click Delete.
      The Delete Browsing History window opens.
   c. Select Temporary Internet files and website files, and Cookies and Website data.
   d. Click Delete.
      The Delete Browsing History window closes.
   e. Click OK.

3. On Mozilla Firefox®:
   a. Go to Options > Privacy.
   b. Click clear your recent history.
   c. Select Cookies and Cache.
   d. Click Clear now.
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

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:


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:

<table>
<thead>
<tr>
<th>Address</th>
<th>Trend Micro, Incorporated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>225 E. John Carpenter Freeway, Suite 1500</td>
</tr>
<tr>
<td></td>
<td>Irving, Texas 75062 U.S.A.</td>
</tr>
<tr>
<td>Phone</td>
<td>Phone: +1 (817) 569-8900</td>
</tr>
<tr>
<td></td>
<td>Toll-free: (888) 762-8736</td>
</tr>
<tr>
<td>Website</td>
<td><a href="http://www.trendmicro.com">http://www.trendmicro.com</a></td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:support@trendmicro.com">support@trendmicro.com</a></td>
</tr>
</tbody>
</table>

- Worldwide support offices:
- 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:

File Reputation Services

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


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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Type the logon credentials (user name and password) for the management console.</td>
</tr>
</tbody>
</table>
| Password    | 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. |
| Session duration | Choose how long you would like to be logged on.  
  • Default: 10 minutes  
  • Extended: 1 day  
  To change these values, 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, in Administration > Accounts / Contacts, to create and manage user accounts. Users can use these accounts, instead of the default administrator account, to access the management console.

Some settings are shared by all user accounts, while others are specific to each account.
This screen includes the following options.

**TABLE A-2. Accounts Tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Click <strong>Add</strong> to add a new user account. This opens the <strong>Add Account</strong> window, where you specify settings for the account. For details, see <strong>Add Account Window on page A-5</strong>.</td>
</tr>
<tr>
<td>Edit</td>
<td>Select a user account and then click <strong>Edit</strong> to edit its settings. This opens the <strong>Edit Account</strong> window, which contains the same settings as the <strong>Add Account</strong> window. For details, see <strong>Add Account Window on page A-5</strong>. Only one user account can be edited at a time.</td>
</tr>
<tr>
<td>Delete</td>
<td>Select one or more user accounts to delete and then click <strong>Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td>• You cannot delete the default Deep Discovery Analyzer administrator account.</td>
</tr>
<tr>
<td></td>
<td>• You cannot delete the logged-on account.</td>
</tr>
<tr>
<td>Unlock</td>
<td>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. Accounts locked this way, including administrator accounts, unlock automatically after ten minutes. The administrator can manually unlock accounts that have been locked. Only one user account can be unlocked at a time.</td>
</tr>
<tr>
<td>Sort Column Data</td>
<td>Click a column title to sort the data below it.</td>
</tr>
<tr>
<td>Search</td>
<td>If there are many entries in the table, type some characters in the <strong>Search</strong> 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 table for matches.</td>
</tr>
</tbody>
</table>
Getting Started

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records and Pagination Controls</td>
<td>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.</td>
</tr>
</tbody>
</table>

Add Account Window

The **Add Account** window appears when you click **Add** on the **Accounts** tab.

![Add Account Window](image)

- **Name:**

- **User name:**

- **Password:**
  - **Password policy:** Type a password that contains at least 8 characters and includes uppercase letters, lowercase letters, numbers, and special characters.

- **Confirm password:**

- **Description:**

- **Role:**
  - **Administrator**
    - Full access to submitted objects, analysis results, and product settings
  - **Investigator**
    - Submit objects to analyze
    - Read-only access to submitted objects, analysis results, and product settings
  - **Operator**
    - Read-only access to submitted objects, analysis results, and product settings

- **Add to contacts**

- **Email address:**

- **Phone number:**

  ![Save and Cancel buttons](image)
This window includes the following options.

**TABLE A-3. Add Account Window**

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type the name of the account owner.</td>
</tr>
<tr>
<td>User name and password</td>
<td>Type an account name that does not exceed 40 characters. Type a password with at least eight characters and then confirm it. If you want to use a stricter password, configure the global password policy in Administration &gt; System Settings &gt; Password Policy tab. The password policy will be 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.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Type a description that does not exceed 40 characters.</td>
</tr>
<tr>
<td>Role</td>
<td>Select the role and associated permissions of this user account.</td>
</tr>
<tr>
<td></td>
<td>• Administrator: Users have full access to submitted objects, analysis results, and product settings</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• Operator: Users have read-only access to submitted objects, analysis results, and product settings</td>
</tr>
<tr>
<td>Add to contacts</td>
<td>Select to add this user account to the Contacts list.</td>
</tr>
<tr>
<td>Email address</td>
<td>Type the email address of the account owner.</td>
</tr>
<tr>
<td>Phone number</td>
<td>(Optional) Type the phone number of the account owner.</td>
</tr>
</tbody>
</table>
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-13.

5. Configure SMTP settings to enable sending of notifications through email. For details, see SMTP Tab on page A-15.

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.


For details, see the Deep Discovery Analyzer 5.8 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 5.8 Administrator's Guide.
License

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

<table>
<thead>
<tr>
<th>Product Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product name:</td>
</tr>
<tr>
<td>Firmware version:</td>
</tr>
<tr>
<td>License agreement:</td>
</tr>
</tbody>
</table>

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-4. Product Details**

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product name</td>
<td>Displays the name of the product.</td>
</tr>
<tr>
<td>Firmware version</td>
<td>Displays the full build number of the product.</td>
</tr>
<tr>
<td>License agreement</td>
<td>Displays a link to the Trend Micro License Agreement. Click the link to view or print the license agreement.</td>
</tr>
</tbody>
</table>

**TABLE A-5. License Details**

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Code</td>
<td>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.</td>
</tr>
</tbody>
</table>

![Activation Code](image)

The License screen reappears displaying the number of days left before the product 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.

<table>
<thead>
<tr>
<th><strong>System Settings</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Proxy SMTP</td>
</tr>
<tr>
<td>Time SNMP</td>
</tr>
<tr>
<td>Password Policy</td>
</tr>
<tr>
<td>Session Timeout</td>
</tr>
<tr>
<td>Cluster High Avail.</td>
</tr>
</tbody>
</table>

**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.

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 4-4.

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.

The following table lists configuration limitations.

**Table A-6. Configuration Limitations**

<table>
<thead>
<tr>
<th>Field</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Cannot be modified when using high availability</td>
</tr>
<tr>
<td>IPv4 address</td>
<td>• Must differ from IPv4 virtual address</td>
</tr>
<tr>
<td></td>
<td>• Must be in the same network segment as IPv4 virtual address</td>
</tr>
<tr>
<td>IPv6 address</td>
<td>• Must differ from IPv6 virtual address</td>
</tr>
<tr>
<td></td>
<td>• Must be in the same network segment as IPv6 virtual address</td>
</tr>
<tr>
<td></td>
<td>• Cannot be deleted if IPv6 virtual address has been configured</td>
</tr>
<tr>
<td></td>
<td>• Cannot be added or deleted when using high availability</td>
</tr>
</tbody>
</table>
Proxy Tab

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

**System Settings**

<table>
<thead>
<tr>
<th>Network</th>
<th>Proxy</th>
<th>SMTP</th>
<th>Time</th>
<th>SNMP</th>
<th>Password Policy</th>
<th>Session Timeout</th>
<th>Cluster</th>
<th>High Availability</th>
</tr>
</thead>
</table>

- **Use an HTTP proxy server**
  - Server name or IP address: [Enter]
  - Port: [Enter]

- **Proxy server requires authentication**
  - User name: [Enter]
  - Password: [Enter]

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an HTTP proxy server</td>
<td>Select this option to enable proxy settings.</td>
</tr>
<tr>
<td>Server name or IP address</td>
<td>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.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port number that Deep Discovery Analyzer uses to connect to the proxy server.</td>
</tr>
</tbody>
</table>
### 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
- NTMLv1 authentication

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy server requires authentication</td>
<td>Select this option if the connection to the proxy server requires authentication. Deep Discovery Analyzer supports the following authentication methods:</td>
</tr>
</tbody>
</table>
- No authentication
- Basic authentication
- Digest authentication
- NTMLv1 authentication |

<table>
<thead>
<tr>
<th>User name</th>
<th>Type the user name used for authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>This option is only available if Proxy server requires authentication is enabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Password</th>
<th>Type the password used for authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>This option is only available if Proxy server requires authentication is enabled.</td>
</tr>
</tbody>
</table>

### 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.

![Time settings panel](image)

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

The settings panel appears.

![Set date and time](image)

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**.
Getting Started

The settings panel appears.

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.

9. Select the preferred date and time format.

10. Click **Save**.

**SMTP Tab**

Deep Discovery Analyzer uses SMTP settings when sending notifications through email.
1. Go to Administration > System Settings and click the SMTP tab.

2. Specify the following details:

**Table A-8. SMTP Tab Tasks**

<table>
<thead>
<tr>
<th><strong>FIELD</strong></th>
<th><strong>STEPS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server address</td>
<td>Type the SMTP server host name, IPv4 address, or IPv6 address.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Port</td>
<td>Type the port number used by the SMTP server.</td>
</tr>
<tr>
<td>Connection security</td>
<td>Specify the type of security used for the connection.</td>
</tr>
<tr>
<td></td>
<td>Available values are: None, STARTTLS, SSL/TLS.</td>
</tr>
<tr>
<td>Sender email address</td>
<td>Type the email address of the sender.</td>
</tr>
<tr>
<td></td>
<td>The default value is <a href="mailto:notifications@ddan.local">notifications@ddan.local</a>.</td>
</tr>
</tbody>
</table>
A-17

<table>
<thead>
<tr>
<th>FIELD</th>
<th>STEPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP server requires authentication</td>
<td>If the server requires authentication, select <strong>SMTP server requires authentication</strong> and specify a user name and password.</td>
</tr>
</tbody>
</table>

**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**

The hardware specifications of your product determine the number of images that you can import and the number of instances that you can deploy per image.

Virtual Analyzer supports OVA files up to 20GB 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.

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.

---

**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 or 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**:

  - **Save** | **Test Internet Connectivity**
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-9. Cluster Configurations**

<table>
<thead>
<tr>
<th>Cluster Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High availability cluster</td>
<td>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.</td>
</tr>
<tr>
<td>Load-balancing cluster</td>
<td>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.</td>
</tr>
<tr>
<td>High availability cluster with load balancing</td>
<td>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.</td>
</tr>
</tbody>
</table>

The following table lists the available configuration modes and associated appliance behavior.
<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary (Active)</td>
<td>• Management console is fully accessible</td>
</tr>
<tr>
<td></td>
<td>• Retains all configuration settings</td>
</tr>
<tr>
<td>Primary (Passive)</td>
<td>• Management console is unavailable</td>
</tr>
<tr>
<td></td>
<td>• Automatically configured based on the settings of the active</td>
</tr>
<tr>
<td></td>
<td>• On standby</td>
</tr>
<tr>
<td></td>
<td>• Takes over as the active primary appliance if the active</td>
</tr>
<tr>
<td></td>
<td>• Does not process submissions</td>
</tr>
<tr>
<td></td>
<td>• primary appliance encounters an error and is unable to</td>
</tr>
<tr>
<td></td>
<td>• recover</td>
</tr>
</tbody>
</table>

**TABLE A-10. Cluster Configuration Modes**
### 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 > Cloud Sandbox
  - 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-11. Nodes List Columns**

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Connection status of the appliance. Mouseover a status icon to view details.</td>
</tr>
<tr>
<td>Mode</td>
<td>Cluster mode of the appliance.</td>
</tr>
<tr>
<td>Management IP Address</td>
<td>Management IP address of the appliance.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host name of the appliance.</td>
</tr>
<tr>
<td>Last Connected</td>
<td>Date and time that the appliance last connected to the active primary appliance.</td>
</tr>
</tbody>
</table>

**Note**
No data (indicated by a dash) if appliance is passive primary appliance.
## Getting Started

<table>
<thead>
<tr>
<th><strong>Column</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details</strong></td>
<td>Additional details about the operational status of the appliance.</td>
</tr>
<tr>
<td></td>
<td>• For standalone appliance:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Standalone appliance</strong>: The appliance is a standalone appliance.</td>
</tr>
<tr>
<td></td>
<td>• For passive primary appliance:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fully synced</strong>: The passive primary appliance is fully synced to the active primary appliance.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Syncing n%</strong>: The passive primary appliance is syncing settings from the active primary appliance.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sync error</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>• For secondary appliances:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Inconsistent component version</strong>: One or more components have different versions on the active primary appliance and secondary appliance. Use the same component versions on all appliances.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not connected</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Invalid API key</strong>: The secondary appliance is configured with an invalid API key. Verify the <strong>Active primary API key</strong> on the secondary appliance.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Incompatible software version</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unexpected error</strong>: An unexpected error has occurred. If the issue persists, contact your support provider.</td>
</tr>
</tbody>
</table>
### Column Description

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td>Actions that can be executed depending on the appliance mode and status.</td>
</tr>
<tr>
<td></td>
<td>• For active primary appliance:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Swap</strong>: Swap the roles of the primary appliances. Sets the current</td>
</tr>
<tr>
<td></td>
<td>passive primary appliance to primary mode (active) and the current</td>
</tr>
<tr>
<td></td>
<td>active primary appliance to primary mode (passive). Appears when the</td>
</tr>
<tr>
<td></td>
<td>passive primary appliance has synced all settings from the active</td>
</tr>
<tr>
<td></td>
<td>primary appliance. For details, see *Swapping the Active Primary</td>
</tr>
<tr>
<td></td>
<td>Appliance and the Passive Primary Appliance on page A-29*</td>
</tr>
<tr>
<td></td>
<td>• For passive primary appliance:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Detach</strong>: Detach the passive primary appliance. Disables high</td>
</tr>
<tr>
<td></td>
<td>availability and allows the passive primary appliance to be used as a</td>
</tr>
<tr>
<td></td>
<td>standalone appliance. Appears when the passive primary appliance has</td>
</tr>
<tr>
<td></td>
<td>synced all settings from the active primary appliance. For details, see</td>
</tr>
<tr>
<td></td>
<td><em>Detaching the Passive Primary Appliance from the Cluster on page A-29</em></td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove</strong>: Remove inaccessible passive primary appliance. Disables high</td>
</tr>
<tr>
<td></td>
<td>availability. Appears when the active primary appliance is unable to</td>
</tr>
<tr>
<td></td>
<td>reach the passive primary appliance through eth3. For details, see</td>
</tr>
<tr>
<td></td>
<td><em>Removing the Passive Primary Appliance from the Cluster on page A-29</em></td>
</tr>
<tr>
<td></td>
<td>• For secondary appliances:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove</strong>: Remove inaccessible secondary appliance. Affects object</td>
</tr>
<tr>
<td></td>
<td>processing capacity. Secondary appliances attempt to connect to the</td>
</tr>
<tr>
<td></td>
<td>active primary appliance every 10 seconds. Appears when the active</td>
</tr>
<tr>
<td></td>
<td>primary appliance does not receive a heartbeat from the secondary</td>
</tr>
<tr>
<td></td>
<td>appliance within one minute. For details, see *Removing a Secondary</td>
</tr>
<tr>
<td></td>
<td>Appliance from the Cluster on page A-32*</td>
</tr>
</tbody>
</table>

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-12. High Availability Clustering Requirements**

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

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 Control Manager, only register the active primary appliance to Control Manager.
- 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 Control Manager, only register the active primary appliance to Control Manager.
- 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 cloud sandbox 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-13. Example Configuration Using Two Images**

<table>
<thead>
<tr>
<th>Deep Discovery Analyzer Hardware Model</th>
<th>Maximum Number of Instances (Total)</th>
<th>Number of Windows 7 Instances</th>
<th>Number of Windows 8.1 Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>1100</td>
<td>60</td>
<td>40</td>
<td>20</td>
</tr>
<tr>
<td>1000</td>
<td>33</td>
<td>22</td>
<td>11</td>
</tr>
</tbody>
</table>

---

**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-27*.

---

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

**Note**

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

A
account management, A-3
Activation Code, A-8

C
custom network, 2-8
custom port, 2-9

D
deployment tasks
  hardware setup, 3-2
  installation, 3-6
documentation feedback, 6-6

E
Ethernet cables, 2-10

F
form factor, 2-2

G
getting started tasks, A-7

I
images, A-17
installation tasks, 3-2
IP addresses (for product), 2-9

L
license, A-8

M
management console, A-2
management console accounts, A-3
management network, 2-8
management port, 2-9

N
network environment, 2-8

P
port, 2-9
ports, 2-11
power supply, 3-2
preconfiguration console, 4-2
  operations, 4-3
product specifications, 2-2

S
sandbox images, A-17
sandbox management
  images
    importing, A-17
  network connection, A-19
session duration (for management console), A-3
support
  resolve issues faster, 6-4
system maintenance
  cluster tab
    primary appliance, A-33
    remove, A-32
  test connection, A-30
nodes list, A-23
system settings
  Network Tab, A-10
  Proxy Tab, A-12
  Time Tab, A-13