TREND MICRO™

5.5 TREND MICRO™ TippingPoint™ Advanced Threat Protection Analyzer

Service Pack 1

Installation and Deployment Guide

Breakthrough Protection Against APTs and Targeted Attacks

Endpoint Security

Network Security

Protected Cloud

TREND MICRO SMART Protection Network™

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/enterprise/tippingpoint-advanced-threat-protection-analyzer.aspx

Document Part No.: APEM57454/160713

Release Date: August 2016

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

Chapter 1: Introduction

Chapter 2: Preparing to Deploy TippingPoint Advanced Threat Protection Analyzer

Chapter 3: Installing the Appliance

Chapter 4: Using the Preconfiguration Console

Chapter 5: Migration

Chapter 6: Technical Support

Appendix A: Getting Started

Index

Preface

Preface

Welcome to the Trend Micro™ TippingPoint™ Advanced Threat Protection Analyzer *Installation and Deployment Guide*. This guide contains information about the requirements and procedures for deploying, installing and migrating TippingPoint ATP Analyzer.

Documentation

The documentation set for TippingPoint Advanced Threat Protection Analyzer includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Administrator's Guide contains detailed instructions on how to configure and manage TippingPoint ATP Analyzer, and explanations on TippingPoint ATP Analyzer concepts and features.
Installation and Deployment Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing TippingPoint ATP Analyzer, and using the Preconfiguration Console to set initial configurations and perform system tasks.
Syslog Content Mapping Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in TippingPoint ATP Analyzer.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting TippingPoint ATP Analyzer to your network and on performing the initial configuration.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.

Document	Description
Online Help	Web-based documentation that is accessible from the TippingPoint ATP Analyzer management console. The Online Help contains explanations of TippingPoint ATP Analyzer components and features, as well as procedures needed to configure TippingPoint ATP Analyzer.
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: http://esupport.trendmicro.com

View and download product documentation from the Trend Micro Online Help Center:

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

Audience

The TippingPoint Advanced Threat Protection Analyzer documentation is written for IT administrators and security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, including the following topics:

- Network topologies
- Database management
- Antivirus and content security protection

The documentation does not assume the reader has any knowledge of sandbox environments or threat event correlation.

Document Conventions

The documentation uses the following conventions:

Table 2. Document Conventions

Convention	Description
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes
Tip	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

Terminology

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

Terminology	Description
Active primary appliance	Clustered appliance with which all management tasks are performed. Retains all configuration settings and allocates submissions to secondary appliances for performance improvement.
Administrator	The person managing TippingPoint Advanced Threat Protection Analyzer
Clustering	Multiple standalone TippingPoint Advanced Threat Protection Analyzer appliances can be deployed and configured to form a cluster that provides fault tolerance, improved performance, or a combination thereof.
Custom port	A hardware port that connects TippingPoint Advanced Threat Protection Analyzer to an isolated network dedicated to sandbox analysis
Dashboard	UI screen on which widgets are displayed
High availability cluster	In a high availability cluster, one appliance acts as the active primary appliance, and one acts as the passive primary appliance. The passive primary appliance automatically takes over as the new active primary appliance if the active primary appliance encounters an error and is unable to recover.
Load-balancing cluster	In a load-balancing cluster, one appliance acts as the active primary appliance, and any additional appliances act as secondary appliances. The secondary appliances process submissions allocated by the active primary appliance for performance improvement.
Management console	A web-based user interface for managing a product.
Management port	A hardware port that connects to the management network.
Passive primary appliance	Clustered appliance that is on standby until active primary appliance encounters an error and is unable to recover. Provides high availability.

Terminology	Description
Role-based administration	Role-based administration streamlines how administrators configure user accounts and control access to the management console.
Sandbox image	A ready-to-use software package (operating system with applications) that require no configuration or installation. Virtual Analyzer supports only image files in the Open Virtual Appliance (OVA) format.
Sandbox instance	A single virtual machine based on a sandbox image.
Secondary appliance	Clustered appliance that processes submissions allocated by the active primary appliance for performance improvement.
Standalone appliance	Appliance that is not part of any cluster. Clustered appliances can revert to being standalone appliances by detaching the appliance from its cluster.
Threat Connect	Correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network. The resulting intelligence reports enable you to investigate potential threats and take actions pertinent to your attack profile.
Virtual Analyzer	An isolated virtual environment used to manage and analyze samples. Virtual Analyzer observes sample behavior and characteristics, and then assigns a risk level to the sample.
Widget	A customizable screen to view targeted, selected data sets.
YARA	YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to your environment.

About Trend Micro

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

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

http://www.trendmicro.com

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

Chapter 1

Introduction

This chapter introduces TippingPoint Advanced Threat Protection Analyzer 5.5 SP1 and the new features in this release.

About TippingPoint Advanced Threat Protection Analyzer

TippingPoint Advanced Threat Protection Analyzer is a custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products. TippingPoint Advanced Threat Protection 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 TippingPoint Advanced Threat Protection 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 1-1. What's New in TippingPoint Advanced Threat Protection Analyzer 5.5 SP1

FEATURE/ENHANCEMENT	DETAILS
Simple Network Management Protocol (SNMP) support	TippingPoint ATP Analyzer sends SNMP trap messages to notify administrators about events that require attention, and listens to SNMP manager requests for system information, status updates, and configuration.
Smart Protection Server integration	TippingPoint ATP Analyzer integrates with Smart Protection Server for web reputation data, and can also use the Smart Protection Server to connect to global services.
Enhanced syslog integration	TippingPoint ATP Analyzer now allows the customization of logs by selecting the scope and exclusions, and provides the option of sending logs to the syslog server using the SSL protocol.

FEATURE/ENHANCEMENT	DETAILS
Threat Types widget	The Threat Types widget shows the type, amount, and risk level of threats detected in all submissions.
Improved detection	TippingPoint ATP Analyzer provides increased protection by improving its detection capabilities. This release supports the deployment of sandbox images running Windows 10, Windows Server 2012 and Windows Server 2012 R2 operating systems.
Network Services Diagnostics	TippingPoint ATP Analyzer provides the option of testing the connectivity of enabled local and global services.
Inline migration from TippingPoint ATP Analyzer 5.5	TippingPoint ATP Analyzer provides users with the option of automatically migrating the settings from 5.5 to 5.5 SP1 using the Firmware screen of the management console.
Improved usability	TippingPoint ATP Analyzer provides improved usability by rearranging several configuration screens, including Cluster and High Availability, and by introducing a new Integrated Products and Services section, which contains the Log Settings, Smart Protection, and Deep Discovery Director screens.

Features and Benefits

TippingPoint Advanced Threat Protection Analyzer includes the following features:

- *Enable Sandboxing as a Centralized Service on page 1-4*
- *Custom Sandboxing on page 1-4*
- *Broad File Analysis Range on page 1-4*
- *YARA Rules on page 1-4*
- *Document Exploit Detection on page 1-5*
- *Automatic URL Analysis on page 1-5*
- *Detailed Reporting on page 1-5*

- *Alert Notifications on page 1-5*
- *Clustered Deployment on page 1-5*
- *Trend Micro Integration on page 1-5*
- *Web Services API and Manual Submission on page 1-6*
- *Custom Defense Integration on page 1-6*

Enable Sandboxing as a Centralized Service

TippingPoint Advanced Threat Protection Analyzer ensures optimized performance with a scalable solution able to keep pace with email, network, endpoint, and any additional source of samples.

Custom Sandboxing

TippingPoint Advanced Threat Protection 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

TippingPoint Advanced Threat Protection 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

TippingPoint Advanced Threat Protection 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, TippingPoint Advanced Threat Protection Analyzer discovers malware and exploits that are often delivered in common office documents and other file formats.

Automatic URL Analysis

TippingPoint Advanced Threat Protection Analyzer performs page scanning and sandbox analysis of URLs that are automatically submitted by integrating products.

Detailed Reporting

TippingPoint Advanced Threat Protection 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 TippingPoint Advanced Threat Protection Analyzer.

Clustered Deployment

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

Trend Micro Integration

TippingPoint Advanced Threat Protection 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

TippingPoint Advanced Threat Protection Analyzer allows any security product or authorized threat researcher to submit samples.

Custom Defense Integration

TippingPoint Advanced Threat Protection Analyzer shares new IOC detection intelligence automatically with other Trend Micro solutions and third-party security products.

Chapter 2

Preparing to Deploy TippingPoint Advanced Threat Protection Analyzer

This chapter discusses the items you need to prepare to deploy TippingPoint Advanced Threat Protection Analyzer and connect it to your network.

If TippingPoint Advanced Threat Protection Analyzer is already deployed on your network and you have a patch or hotfix to apply to it, see the *TippingPoint Advanced Threat Protection Analyzer Administrator's Guide*.

Deployment Overview

Product Specifications

Standard TippingPoint Advanced Threat Protection Analyzer appliances have the following specifications.

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

Product Specifications - 1100 Appliance

FEATURE	SPECIFICATIONS
Rack size	2U 19-inch standard rack
Availability	Raid 1 configuration
Storage size	4 TB free storage
Connectivity	• Management port: 1 x 10Base-T/100Base-TX/ 1000Base-T • Custom ports: 3 x 10Base-T/100Base-TX/1000Base-T
Dimensions (WxDxH)	48.2 cm (18.98 in) x 75.58 cm (29.75 in) x 8.73 cm (3.44 in)
Maximum weight	31.5 kg (69.45 lb)
Operating temperature Power	10 °C to 35 °C at 10% to 80% relative humidity (RH) 750W, 120-240 VAC 50/60 Hz

Deployment Considerations

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

Multiple standalone TippingPoint Advanced Threat Protection 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 TippingPoint Advanced Threat Protection Analyzer appliances available, you may deploy the following cluster configurations:

TABLE 2-1. Cluster Configurations

CLUSTER CONFIGURATION	DESCRIPTION
High availability cluster	In a high availability cluster, one appliance acts as the active primary appliance, and one acts as the passive primary appliance. The passive primary appliance automatically takes over as the new active primary appliance if the active primary appliance encounters an error and is unable to recover. For details, see *High Availability Cluster on page 2-4*.
Load-balancing cluster	In a load-balancing cluster, one appliance acts as the active primary appliance, and any additional appliances act as secondary appliances. The secondary appliances process submissions allocated by the active primary appliance for performance improvement. For details, see *Load-Balancing Cluster on page 2-5*.
High availability cluster with load balancing	In a high availability cluster with load balancing, one appliance acts as the active primary appliance, one acts as the passive primary appliance, and any additional appliances act as secondary appliances. The passive primary appliance takes over as the active primary appliance if the active primary appliance encounters an error and is unable to recover. The secondary appliances process submissions allocated by the active primary appliance for performance improvement. For details, see *High Availability Cluster with Load Balancing on page 2-6*.

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 TippingPoint Advanced Threat Protection Analyzer capabilities remain available even when the appliance encounters an error and is unable to recover.

The following figure shows two TippingPoint Advanced Threat Protection Analyzer appliances deployed in a high availability cluster configuration and how integrating products communicate with TippingPoint Advanced Threat Protection 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.

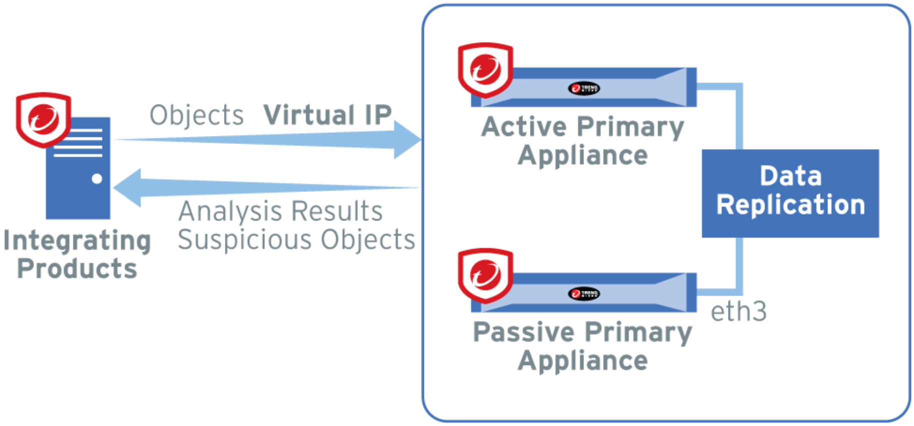


FIGURE 2-1. High Availability Cluster

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 TippingPoint Advanced Threat Protection Analyzer appliances deployed in a load-balancing cluster configuration and how integrating products communicate with TippingPoint Advanced Threat Protection Analyzer.

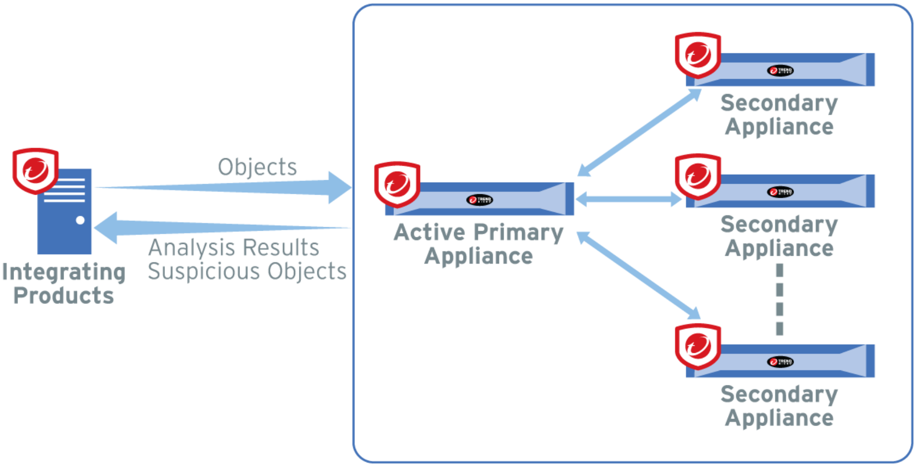


FIGURE 2-2. Load-Balancing Cluster

High Availability Cluster with Load Balancing

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

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

The following figure shows TippingPoint Advanced Threat Protection Analyzer appliances deployed in a high availability cluster configuration and how integrating products communicate with TippingPoint Advanced Threat Protection 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.

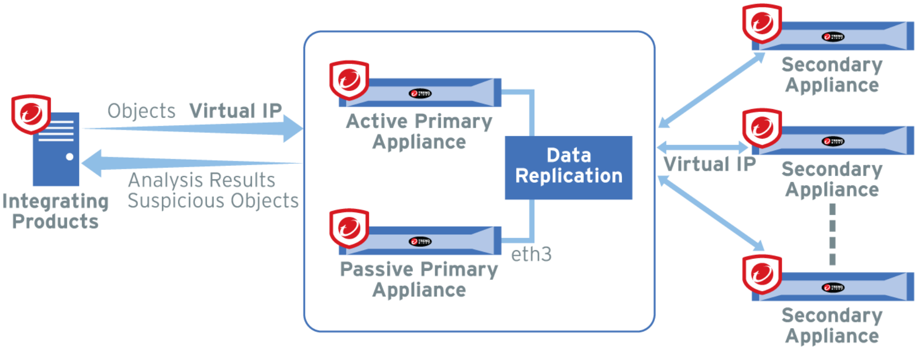


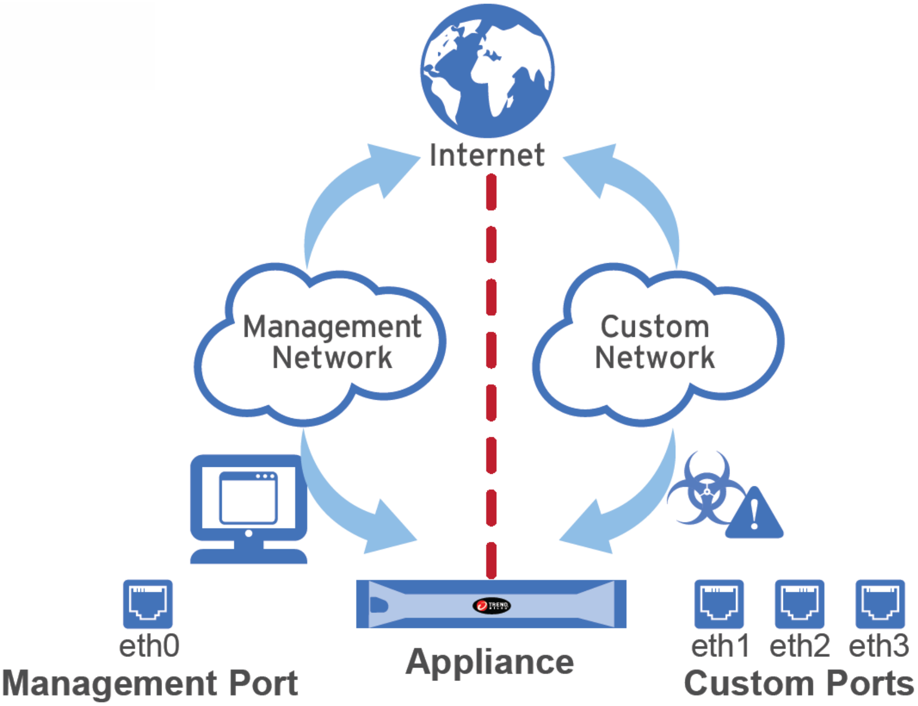
FIGURE 2-3. High Availability Cluster with Load Balancing

Recommended Network Environment

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

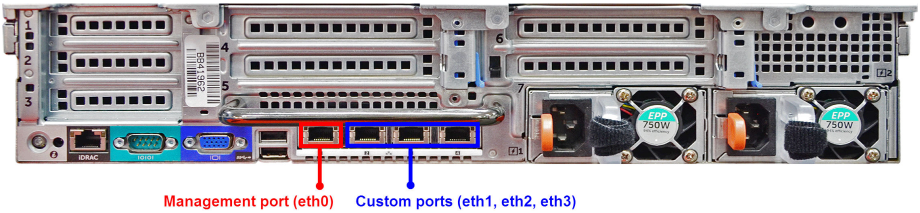
Trend Micro recommends using a custom network for sample analysis. Custom networks ideally are connected to the Internet but do not have proxy settings, proxy authentication, and connection restrictions.

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



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.

TippingPoint ATP 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 TippingPoint Advanced Threat Protection Analyzer *Administrator's Guide*.

Deployment Requirements

Requirement	Details
TippingPoint Advanced Threat Protection Analyzer	Obtain from Trend Micro
TippingPoint Advanced Threat Protection Analyzer installation CD	Obtain from Trend Micro
Activation Code	Obtain from Trend Micro
Monitor and VGA cable	Connects to the VGA port of the appliance
USB keyboard	Connects to a USB port of the appliance
USB mouse	Connects to a USB port of the appliance
Ethernet cables	• One cable connects the management port of the appliance to the management network. • One cable connects a custom port to an isolated network that is reserved for sandbox analysis. • If using high availability, one cable connects eth3 to eth3 on an identical appliance.
Internet-enabled computer	A computer with the following software installed: • Microsoft Internet Explorer™ 9, 10, or 11 • Microsoft Edge™ • Google Chrome™ • Mozilla Firefox™ • Adobe® Flash® 10 or later
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

REQUIREMENT	DETAILS
Third party software licenses	Licenses for all third party software installed on sandbox images

Logon Credentials

CONSOLE	PURPOSE	DEFAULT CREDENTIALS	YOUR INFORMATION
Preconfiguration console	Perform initial configuration tasks. See *Configuring Network Addresses on the Preconfiguration Console on page 4-4*.	• TippingPoint ATP Analyzer **login** (not configurable): `admin` • **Password**: `admin`	**Password**:
Management console	• Configure product settings • View and download reports	• **User name** (not configurable): `admin` • **Password**: `Admin1234!`	**Password**:
		Other user accounts (configured on the management console, in **Administration** > **Accounts / Contacts** > **Accounts**)	User account 1: **User name**: **Password**:
			User account 2: **User name**: **Password**:

Ports Used by the Appliance

The following table shows the ports that are used with TippingPoint Advanced Threat Protection Analyzer and why they are used.

TABLE 2-2. Ports used by TippingPoint ATP Analyzer

PORT	PROTOCOL	FUNCTION	PURPOSE
21	TCP	Outbound	TippingPoint Advanced Threat Protection Analyzer uses this port to send backup data to FTP servers.
22	TCP	Listening and outbound	TippingPoint ATP Analyzer uses this port to: • Access the preconfiguration console with a computer through SSH • Send backup data to an SFTP server
25	TCP	Outbound	TippingPoint ATP Analyzer sends notifications and scheduled reports through SMTP.
53	TCP/UDP	Outbound	TippingPoint ATP Analyzer uses this port for DNS resolution.
67	UDP	Outbound	TippingPoint ATP Analyzer sends requests to the DHCP server if IP addresses are assigned dynamically.
68	UDP	Listening	TippingPoint ATP Analyzer receives responses from the DHCP server.

Port	Protocol	Function	Purpose
80	TCP	Listening and outbound	TippingPoint ATP Analyzer connects to other computers and integrated Trend Micro products and hosted services through this port. In particular,TippingPoint ATP Analyzer uses this port to: • Verify the TippingPoint ATP 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
123	UDP	Listening and outbound	TippingPoint ATP Analyzer connects to the NTP server to synchronize time.
137	UDP	Outbound	TippingPoint ATP Analyzer uses NetBIOS to resolve IP addresses to host names.
161	UDP	Outbound	TippingPoint ATP Analyzer uses this port to send trap messages to SNMP managers.
162	UDP	Listening	TippingPoint ATP Analyzer uses this port to listen for requests from SNMP managers.

Port	Protocol	Function	Purpose
443	TCP	Listening and outbound	TippingPoint ATP Analyzer uses this port to: • Access the management console with a computer through HTTPS • Communicate with other TippingPoint Advanced Threat Protection Analyzer appliances in a cluster environment • Connect to Trend Micro Threat Connect • Communicate with Trend Micro Control Manager • Connect to Web Reputation Services to query the blocking reason • Receive files from a computer with Manual Submission Tool • Receive samples from integrated products • Send anonymous threat information from Smart Feedback • Send Suspicious Objects list and analysis information to integrated products • Update components by connecting to the ActiveUpdate server • Verify the safety of files through the Certified Safe Software Service • Communicate with Deep Discovery Director

Port	Protocol	Function	Purpose
User-defined		Outbound	TippingPoint Advanced Threat Protection Analyzer uses user-defined ports to: • Send logs to syslog servers • Connect to the proxy server • Connect to the Smart Protection Server

Chapter 3

Installing the Appliance

This chapter discusses the TippingPoint Advanced Threat Protection Analyzer installation tasks.

TippingPoint Advanced Threat Protection 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 TippingPoint Advanced Threat Protection Analyzer. For details, see *Installing TippingPoint Advanced Threat Protection 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

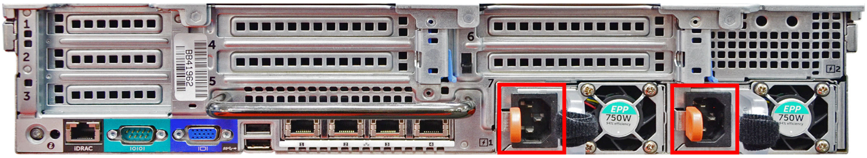
1. Mount the appliance in a standard 19-inch 4-post rack, or on a free-standing object, such as a sturdy desktop.

   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.

   TippingPoint ATP 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.

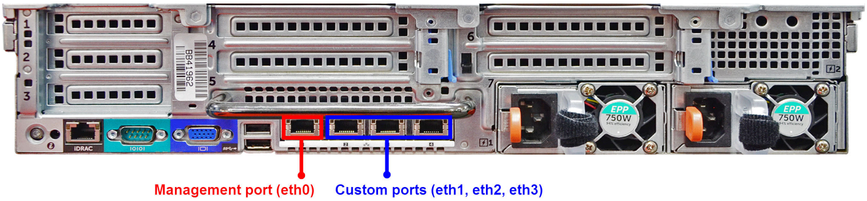
4. Connect the keyboard and mouse to the USB ports at the back of the appliance.

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 TippingPoint Advanced Threat Protection Analyzer

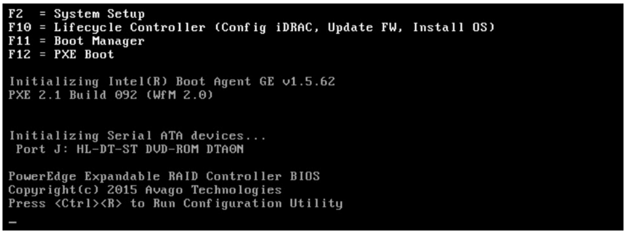
Procedure

1. Power on the appliance.

Note

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

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

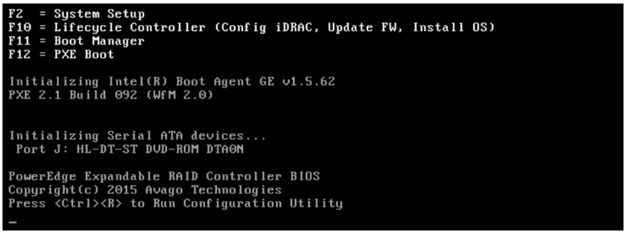


```
F2  = System Setup
F10 = Lifecycle Controller (Config iDRAC, Update FW, Install OS)
F11 = Boot Manager
F12 = PXE Boot

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


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

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

2. Insert the CD containing the TippingPoint Advanced Threat Protection Analyzer installation package.

3. Restart the appliance.

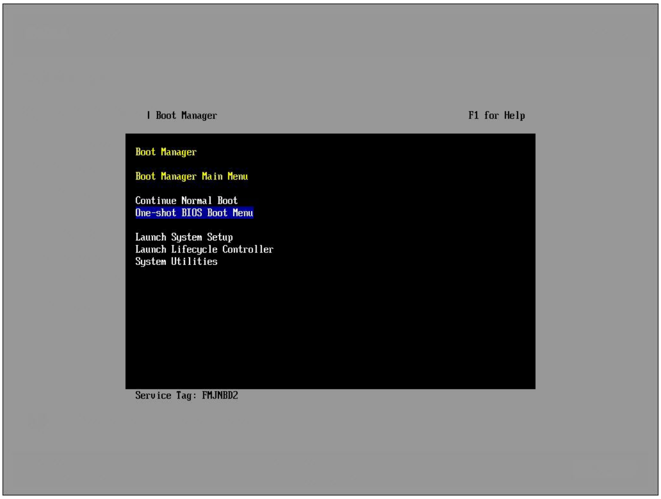
   The **POST** screen appears.



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

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


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

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

4. Press F11.

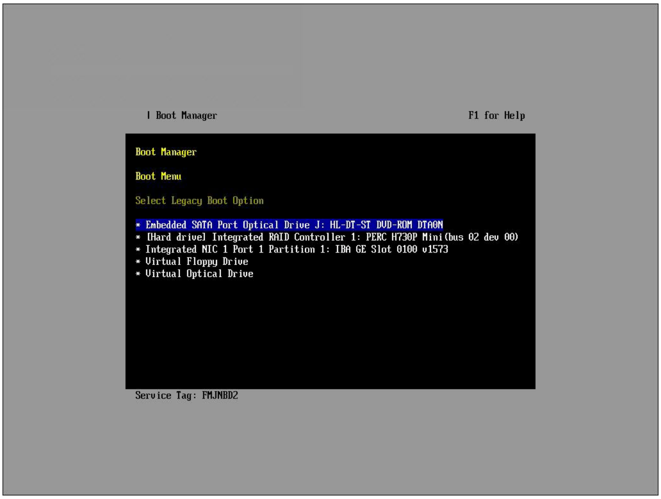
The **Boot Manager** screen appears.



```
 | Boot Manager                                          F1 for Help

Boot Manager

Boot Manager Main Menu

Continue Normal Boot
One-shot BIOS Boot Menu

Launch System Setup
Launch Lifecycle Controller
System Utilities

Service Tag: FMJNBD2
```

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

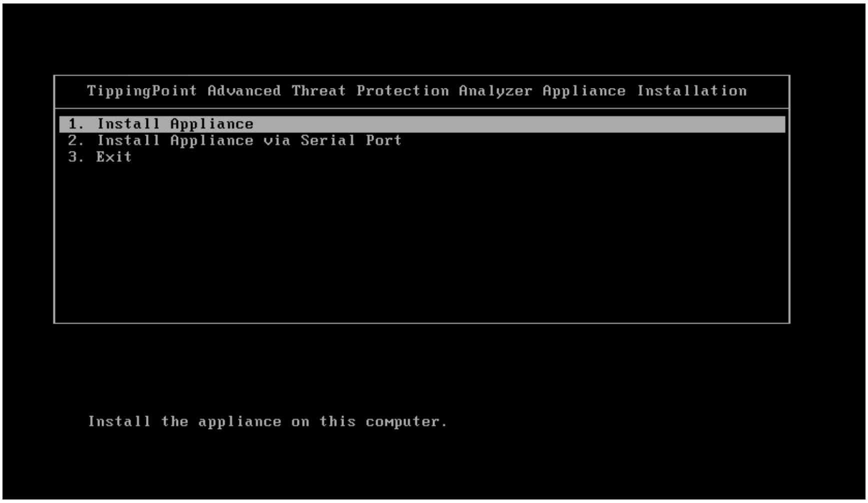
   The **Boot Manager** screen appears.



```
 | Boot Manager                                          F1 for Help

Boot Manager

Boot Menu

Select Legacy Boot Option

* Embedded SATA Port Optical Drive J: HL-DT-ST DVD-ROM DTA0N
* [Hard drive] Integrated RAID Controller 1: PERC H730P Mini(bus 02 dev 00)
* Integrated NIC 1 Port 1 Partition 1: IBA GE Slot 0100 v1573
* Virtual Floppy Drive
* Virtual Optical Drive

Service Tag: FMJNBD2
```

6. Select **DVD-ROM** and press ENTER.

   The **TippingPoint Advanced Threat Protection Analyzer Appliance Installation** screen appears.

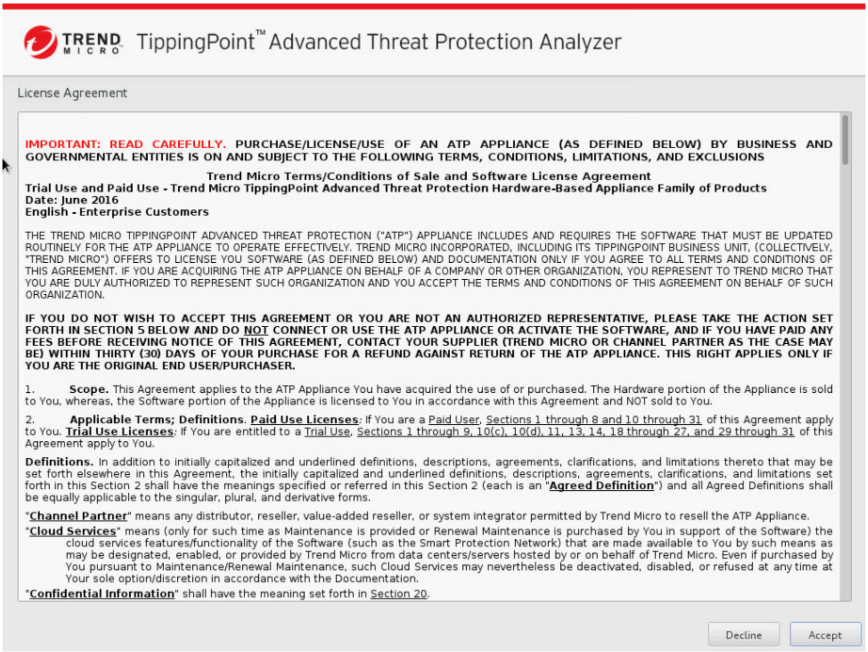


```
TippingPoint Advanced Threat Protection Analyzer Appliance Installation

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

Install the appliance on this computer.
```

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

   - When installing TippingPoint Advanced Threat Protection Analyzer via serial port, select **2. Install Appliance via Serial Port** and press ENTER.

The **License Agreement** screen appears.


TREND MICRO TippingPoint™ Advanced Threat Protection Analyzer
License Agreement

IMPORTANT: READ CAREFULLY. PURCHASE/LICENSE/USE OF AN ATP APPLIANCE (AS DEFINED BELOW) BY BUSINESS AND GOVERNMENTAL ENTITIES IS ON AND SUBJECT TO THE FOLLOWING TERMS, CONDITIONS, LIMITATIONS, AND EXCLUSIONS

Trend Micro Terms/Conditions of Sale and Software License Agreement
Trial Use and Paid Use - Trend Micro TippingPoint Advanced Threat Protection Hardware-Based Appliance Family of Products
Date: June 2016
English - Enterprise Customers

THE TREND MICRO TIPPINGPOINT ADVANCED THREAT PROTECTION ("ATP") APPLIANCE INCLUDES AND REQUIRES THE SOFTWARE THAT MUST BE UPDATED ROUTINELY FOR THE ATP APPLIANCE TO OPERATE EFFECTIVELY. TREND MICRO INCORPORATED, INCLUDING ITS TIPPINGPOINT BUSINESS UNIT, (COLLECTIVELY, "TREND MICRO") OFFERS TO LICENSE YOU SOFTWARE (AS DEFINED BELOW) AND DOCUMENTATION ONLY IF YOU AGREE TO ALL TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU ARE ACQUIRING THE ATP APPLIANCE ON BEHALF OF A COMPANY OR OTHER ORGANIZATION, YOU REPRESENT TO TREND MICRO THAT YOU ARE DULY AUTHORIZED TO REPRESENT SUCH ORGANIZATION AND YOU ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT ON BEHALF OF SUCH ORGANIZATION.

IF YOU DO NOT WISH TO ACCEPT THIS AGREEMENT OR YOU ARE NOT AN AUTHORIZED REPRESENTATIVE, PLEASE TAKE THE ACTION SET FORTH IN SECTION 5 BELOW AND DO NOT CONNECT OR USE THE ATP APPLIANCE OR ACTIVATE THE SOFTWARE, AND IF YOU HAVE PAID ANY FEES BEFORE RECEIVING NOTICE OF THIS AGREEMENT, CONTACT YOUR SUPPLIER (TREND MICRO OR CHANNEL PARTNER AS THE CASE MAY BE) WITHIN THIRTY (30) DAYS OF YOUR PURCHASE FOR A REFUND AGAINST RETURN OF THE ATP APPLIANCE. THIS RIGHT APPLIES ONLY IF YOU ARE THE ORIGINAL END USER/PURCHASER.

1. **Scope.** This Agreement applies to the ATP Appliance You have acquired the use of or purchased. The Hardware portion of the Appliance is sold to You, whereas, the Software portion of the Appliance is licensed to You in accordance with this Agreement and NOT sold to You.

2. **Applicable Terms; Definitions. Paid Use Licenses**: If You are a Paid User, Sections 1 through 8 and 10 through 31 of this Agreement apply to You. **Trial Use Licenses**: If You are entitled to a Trial Use, Sections 1 through 9, 10(c), 10(d), 11, 13, 14, 18 through 27, and 29 through 31 of this Agreement apply to You.

Definitions. In addition to initially capitalized and underlined definitions, descriptions, agreements, clarifications, and limitations thereto that may be set forth elsewhere in this Agreement, the initially capitalized and underlined definitions, descriptions, agreements, clarifications, and limitations set forth in this Section 2 shall have the meanings specified or referred in this Section 2 (each is an "**Agreed Definition**") and all Agreed Definitions shall be equally applicable to the singular, plural, and derivative forms.

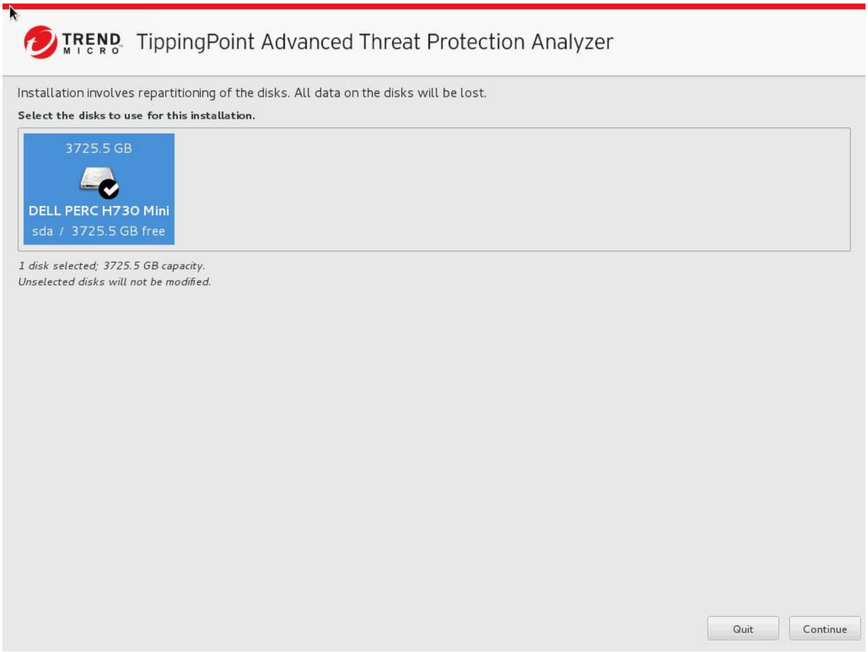
"**Channel Partner**" means any distributor, reseller, value-added reseller, or system integrator permitted by Trend Micro to resell the ATP Appliance.

"**Cloud Services**" means (only for such time as Maintenance is provided or Renewal Maintenance is purchased by You in support of the Software) the cloud services features/functionality of the Software (such as the Smart Protection Network) that are made available to You by such means as may be designated, enabled, or provided by Trend Micro from data centers/servers hosted by or on behalf of Trend Micro. Even if purchased by You pursuant to Maintenance/Renewal Maintenance, such Cloud Services may nevertheless be deactivated, disabled, or refused at any time at Your sole option/discretion in accordance with the Documentation.

"**Confidential Information**" shall have the meaning set forth in Section 20.

8. Click **Accept**.

The **Select Disk** screen appears.



TippingPoint Advanced Threat Protection Analyzer

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

Select the disks to use for this installation.

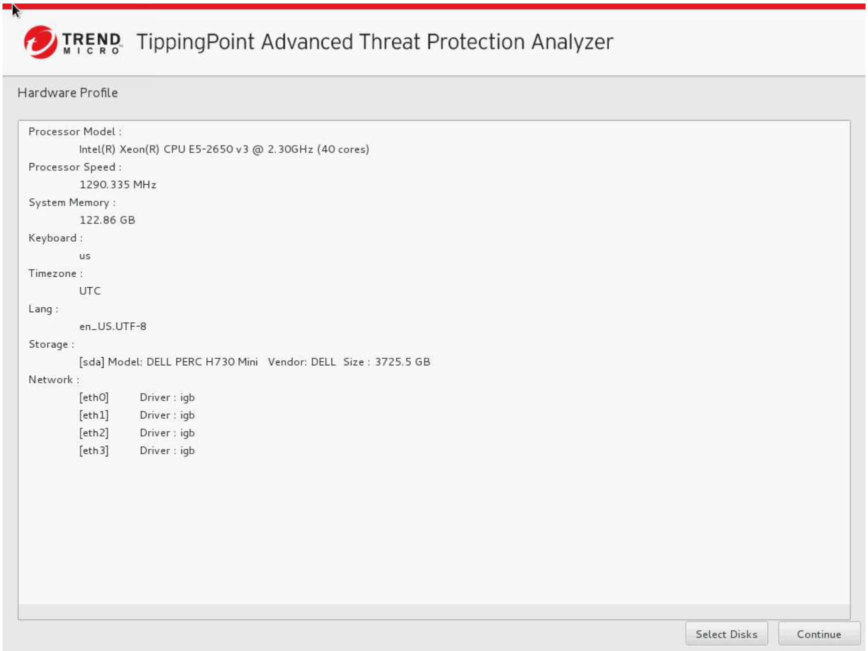
3725.5 GB
DELL PERC H730 Mini
sda / 3725.5 GB free

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

9. Select the disk on which to install the TippingPoint Advanced Threat Protection Analyzer software.

10. Click **Continue**.

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



TippingPoint Advanced Threat Protection Analyzer

Hardware Profile

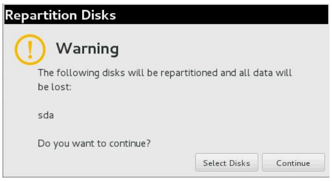
```
Processor Model :
          Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz (40 cores)
Processor Speed :
          1290.335 MHz
System Memory :
          122.86 GB
Keyboard :
          us
Timezone :
          UTC
Lang :
          en_US.UTF-8
Storage :
          [sda] Model: DELL PERC H730 Mini   Vendor: DELL  Size : 3725.5 GB
Network :
          [eth0]      Driver : igb
          [eth1]      Driver : igb
          [eth2]      Driver : igb
          [eth3]      Driver : igb
```

11. Click **Continue**.

WARNING!

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

A confirmation message appears.



Repartition Disks

Warning

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

sda

Do you want to continue?

12. Click **Continue**.

    The installation program repartitions the disks and prepares the environment for installation. Upon completion, the appliance is restarted and TippingPoint Advanced Threat Protection 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*.

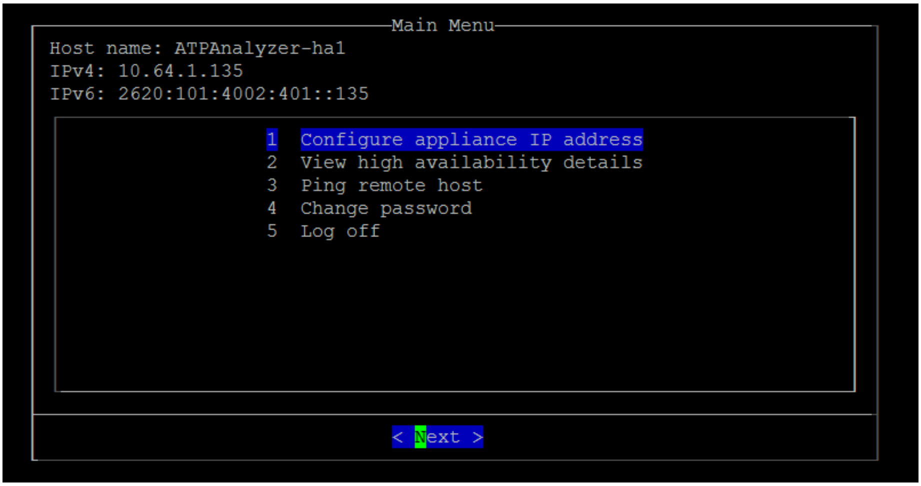
Chapter 4

Using the Preconfiguration Console

This chapter discusses how to use the TippingPoint Advanced Threat Protection 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.



```
                              Main Menu
Host name: ATPAnalyzer-ha1
IPv4: 10.64.1.135
IPv6: 2620:101:4002:401::135

                   1  Configure appliance IP address
                   2  View high availability details
                   3  Ping remote host
                   4  Change password
                   5  Log off

                              < Next >
```

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

Task	Procedure
Logging on	Type valid logon credentials. The default credentials are: • User name: `admin` • Password: `admin`
Configuring network addresses for the appliance	Specify the appliance IP address, subnet mask, gateway, and DNS. For details, see *Configuring Network Addresses on the Preconfiguration Console on page 4-4*.

Task	Procedure
Viewing high availability details	View the active and passive appliance host names, IP addresses, and sync status. **Note** High availability cannot be configured on the preconfiguration console. Use the management console to configure high availability. For details see the *High Availability Tab* and *Cluster Tab* topics in the *TippingPoint Advanced Threat Protection Analyzer Administrator's Guide*.
Pinging a remote host	Type a valid IP address or FQDN and click **Ping**.
Changing the preconfiguration console password	Type the new password twice and click **Save**.
Logging off	On the **Main Menu**, click **Log off**.

Preconfiguration Console Basic Operations

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

Important

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

Keyboard Key	Operation
Up and Down arrows ↑ ↓	Move between fields.
	Move between items in a numbered list. **Note** An alternative way of moving to an item is by typing the item number.
	Move between text boxes.
Left and Right arrows ← →	Move between buttons. Buttons are enclosed in angle brackets <>.
	Move between characters in a text box.
ENTER Enter	Click the highlighted item or button.
TAB Tab ⇆	Move between screen sections, where one section requires using a combination of arrow keys (Up, Down, Left, and Right keys).

Configuring Network Addresses on the Preconfiguration Console

Procedure

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

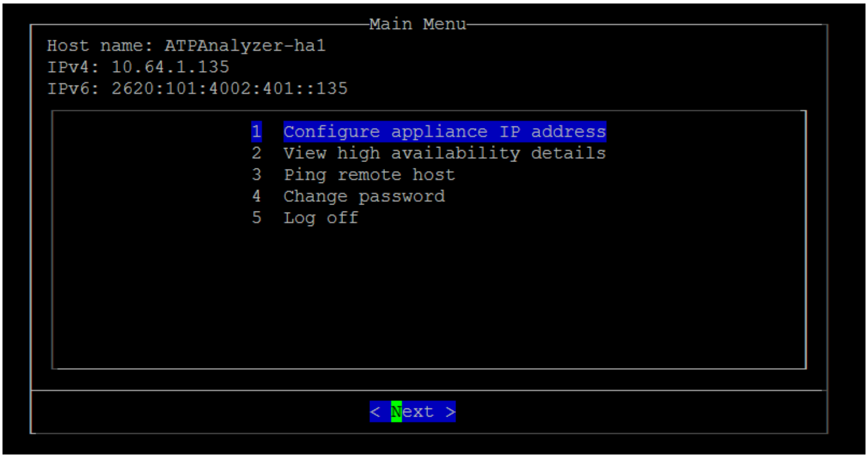
    - User name: `admin`
    - Password: `admin`

Note

None of the characters you type appear on the screen.

This password is different from the password used to log on to the web-based management console. For more information, see *Logon Credentials on page 2-11*.

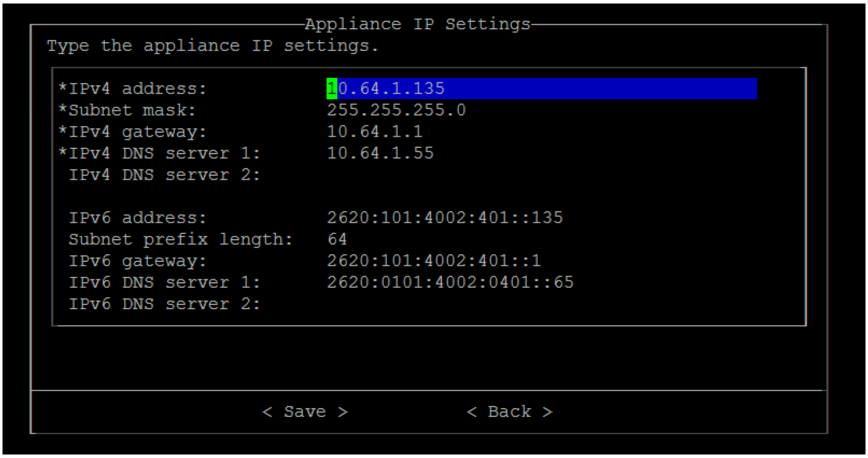
The **Main Menu** screen appears.



```
Main Menu
Host name: ATPAnalyzer-ha1
IPv4: 10.64.1.135
IPv6: 2620:101:4002:401::135

          1   Configure appliance IP address
          2   View high availability details
          3   Ping remote host
          4   Change password
          5   Log off

                    < Next >
```

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

The **Appliance IP Settings** screen appears.



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

 *IPv4 address:            10.64.1.135
 *Subnet mask:             255.255.255.0
 *IPv4 gateway:            10.64.1.1
 *IPv4 DNS server 1:       10.64.1.55
  IPv4 DNS server 2:

  IPv6 address:            2620:101:4002:401::135
  Subnet prefix length:    64
  IPv6 gateway:            2620:101:4002:401::1
  IPv6 DNS server 1:       2620:0101:4002:0401::65
  IPv6 DNS server 2:

                    < Save >           < Back >
```

3. Specify the following required settings:

ITEM	GUIDELINES
IPv4 address	• Must be in the same subnet as the virtual IP address. • Must not conflict with the following addresses: • Sandbox network: Configured in **Virtual Analyzer** > **Sandbox Management** > **Network Connection** • Virtual IP address: Configured in **Administration** > **System Settings** > **High Availability** • Virtual Analyzer: `1.1.0.0` - `1.1.2.255` • Broadcast: `255.255.255.255` • Multicast: `224.0.0.0` - `239.255.255.255` • Link local: `169.254.1.0` - `169.254.254.255` • Class E: `240.0.0.0` - `255.255.255.255` • Localhost: `127.0.0.1/8`

Item	Guidelines
	Note Changing the IP address changes the management console URL.
Subnet mask	Must not be any of the following numbers: • `111.111.111.111` • `255.255.255.255`
IPv4 gateway	Must be in the same subnet as the IP address
IPv4 DNS server 1	Same as IP address
IPv4 DNS server 2 (Optional)	Same as IP address

4. (Optional) Configure the IPv6 settings.

5. Press TAB to navigate to **Save**, and then press ENTER.

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

Viewing High Availability Details on the Preconfiguration Console

Before you begin

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

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

Note

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

Procedure

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

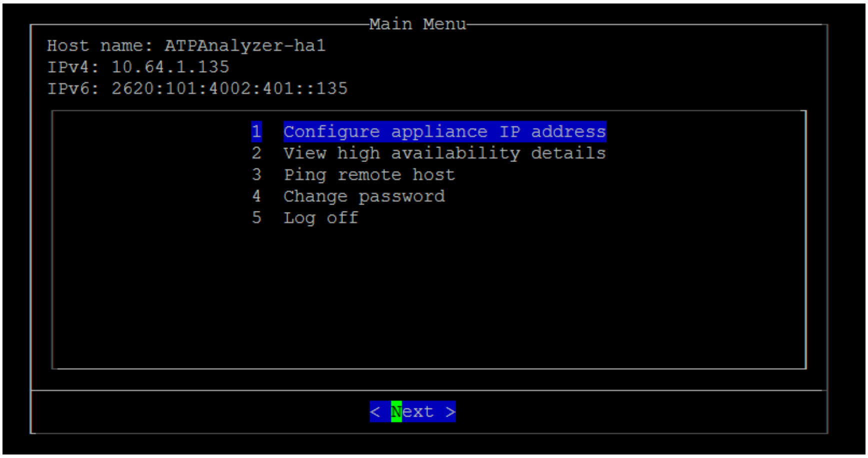
    - User name: `admin`
    - Password: `admin`

    Note

    None of the characters you type appear on the screen.

    This password is different from the password used to log on to the web-based management console. For more information, see *Logon Credentials on page 2-11*.

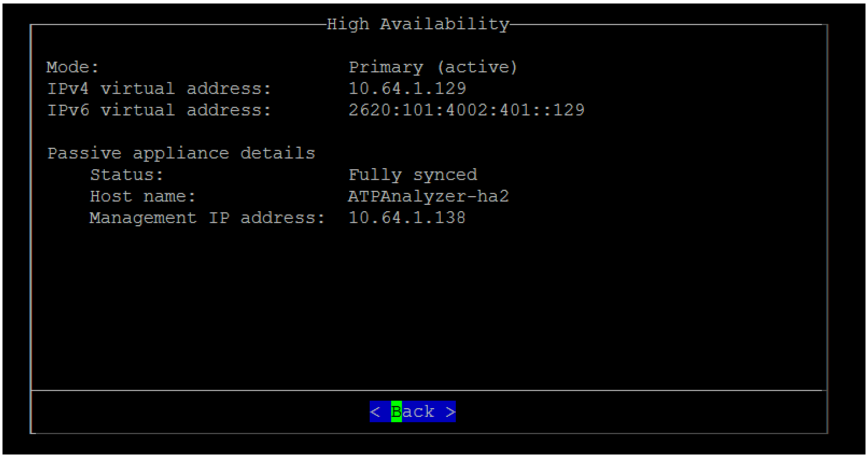
    The **Main Menu** screen appears.



```
Main Menu
Host name: ATPAnalyzer-ha1
IPv4: 10.64.1.135
IPv6: 2620:101:4002:401::135

                   1   Configure appliance IP address
                   2   View high availability details
                   3   Ping remote host
                   4   Change password
                   5   Log off

                            < Next >
```

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

The **High Availability** screen appears.



```
High Availability

Mode:                          Primary (active)
IPv4 virtual address:          10.64.1.129
IPv6 virtual address:          2620:101:4002:401::129

Passive appliance details
    Status:                    Fully synced
    Host name:                 ATPAnalyzer-ha2
    Management IP address:     10.64.1.138
```

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

Table 4-1. High Availability Screen

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

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

Note

Detaching the passive primary appliance disables high availability.

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

   The **Main Menu** screen appears.

Chapter 5

Migration

This chapter discusses how to migrate TippingPoint Advanced Threat Protection Analyzer 5.5 to 5.5 SP1.

Migrating from TippingPoint Advanced Protection Analyzer 5.5 to TippingPoint Advanced Protection Analyzer 5.5 SP1

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

Important

If you have multiple TippingPoint Advanced Threat Protection Analyzer appliances deployed and configured to form a cluster, please perform these tasks:

TABLE 5-1. Cluster Configurations Upgrade Tasks

CLUSTER CONFIGURATION	TASKS
High availability cluster	1. Detach the passive primary appliance. 2. Individually upgrade both the active primary appliance and the passive primary appliance by performing the tasks as described in the main task section below. 3. Add the passive primary appliance to the cluster again.
Load-balancing cluster	Individually upgrade all TippingPoint Advanced Threat Protection Analyzer appliances.
High availability cluster with load balancing	1. Detach the passive primary appliance. 2. Individually upgrade both the active primary appliance and the passive primary appliance by performing the tasks as described in the main task section below. 3. Add the passive primary appliance to the cluster again. 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**.

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

5. Clear the browser cache.

   For details, see *Clearing the Browser Cache on page 5-3*

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

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

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

    Tip

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

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

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

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro TippingPoint Support

Contact the TippingPoint Technical Assistance Center (TAC) by using any of the following options.

Phone	• North America: +1 866 681 8324 • International: +1 512 681 8324 For online support and additional international toll-free numbers, visit https://tmc.tippingpoint.com
Email address	tippingpoint.support@trendmicro.com

- Visit us online at:

  http://www.trendmicro.com/tippingpoint

- Trend Micro product documentation:

  http://docs.trendmicro.com

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

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

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

File Reputation Services

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

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

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

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

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

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

http://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

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

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

Appendix A

Getting Started

This chapter describes how to get started with TippingPoint Advanced Threat Protection Analyzer and configure initial settings.

The Management Console

TippingPoint Advanced Threat Protection Analyzer provides a built-in management console for configuring and managing the product.

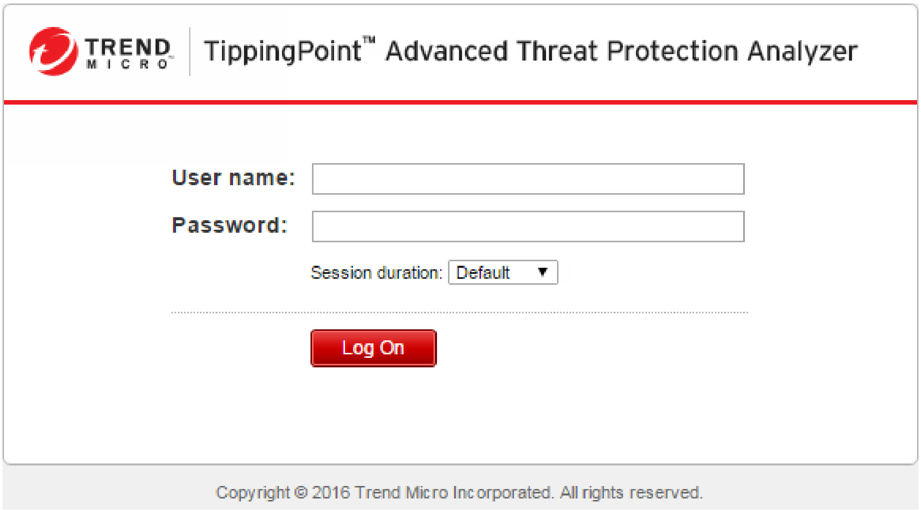
Open the management console from any computer on the management network with the following resources:

- Microsoft Internet Explorer™ 9, 10, or 11
- Microsoft Edge™
- Google Chrome™
- Mozilla Firefox™
- Adobe® Flash® 10 or later

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:


TREND MICRO
TippingPoint™ Advanced Threat Protection Analyzer
User name:
Password:
Log On
Copyright © 2016 Trend Micro Incorporated. All rights reserved.

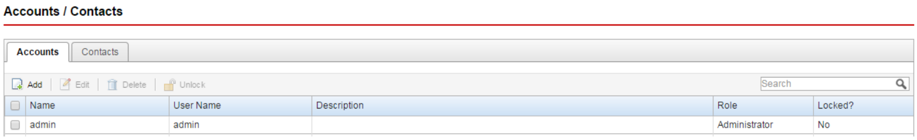
Session duration: Default ▼

Table A-1. Management Console Logon Options

Option	Details
User name Password	Type the logon credentials (user name and password) for the management console. Use the default administrator logon credentials when logging on for the first time: • User name: `admin` • Password: `Admin1234!` Trend Micro recommends changing the password after logging on to the management console for the first time. Configure user accounts to allow other users to access the management console without using the administrator account. For details, see *Accounts Tab on page A-3*.
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.



☐	Name	User Name	Description	Role	Locked?
☐	admin	admin		Administrator	No

Some settings are shared by all user accounts, while others are specific to each account.

This screen includes the following options.

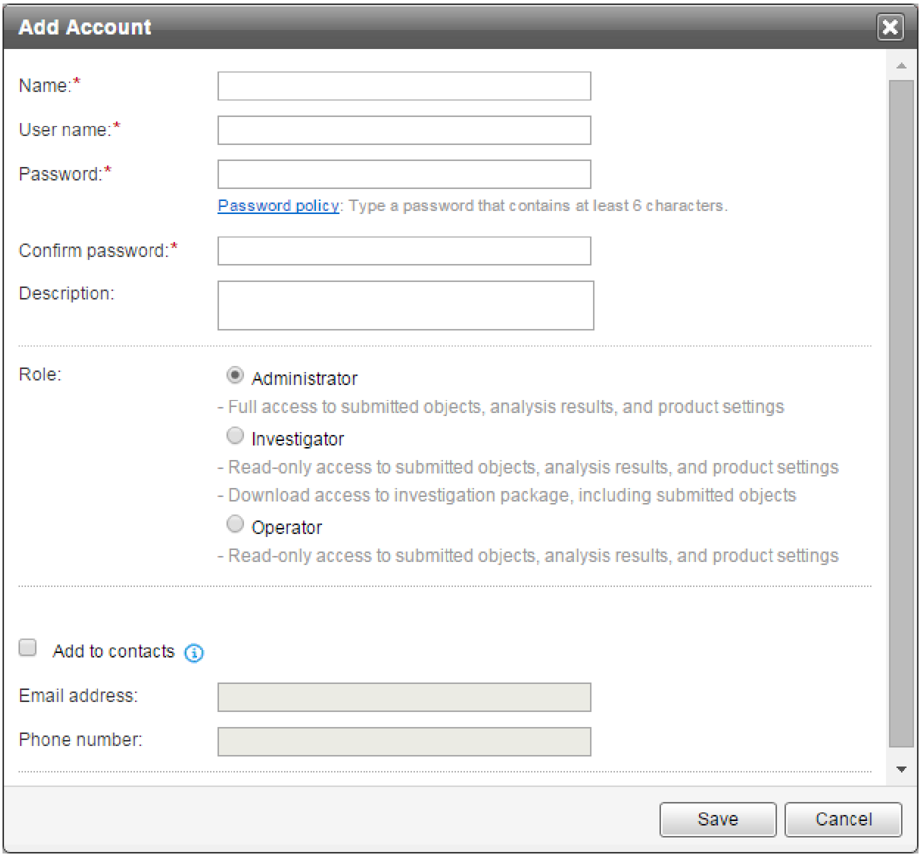
Table A-2. Accounts Tasks

Task	Steps
Add	Click **Add** to add a new user account. This opens the **Add Account** window, where you specify settings for the account. For details, see *Add Account Window on page A-5*.
Edit	Select a user account and then click **Edit** to edit its settings. This opens the **Edit Account** window, which contains the same settings as the **Add Account** window. For details, see *Add Account Window on page A-5*. Only one user account can be edited at a time.
Delete	Select one or more user accounts to delete and then click **Delete**. **Important** • You cannot delete the default TippingPoint Advanced Threat Protection Analyzer administrator account. • You cannot delete the logged-on account.
Unlock	TippingPoint Advanced Threat Protection 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.
Sort Column Data	Click a column title to sort the data below it.
Search	If there are many entries in the table, type some characters in the Search text box to narrow down the entries. As you type, the entries that match the characters you typed are displayed. TippingPoint Advanced Threat Protection Analyzer searches all cells in the table for matches.

TASK	STEPS
Records and Pagination Controls	The panel at the bottom of the screen shows the total number of user accounts. If all user accounts cannot be displayed at the same time, use the pagination controls to view the accounts that are hidden from view.

Add Account Window

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



Add Account

Name:*	
User name:*	
Password:*	
	Password policy: Type a password that contains at least 6 characters.
Confirm password:*	
Description:	

Role:

● Administrator
- Full access to submitted objects, analysis results, and product settings

○ Investigator
- Read-only access to submitted objects, analysis results, and product settings
- Download access to investigation package, including submitted objects

○ Operator
- Read-only access to submitted objects, analysis results, and product settings

□ Add to contacts ⓘ

Email address:	
Phone number:	

This window includes the following options.

TABLE A-3. Add Account Window

FIELD	DETAILS
Name	Type the name of the account owner.
User name and password	Type an account name that does not exceed 40 characters. Type a password with at least six characters and then confirm it. If you want to use a stricter password, configure the global password policy in **Administration** > **System Settings** > **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, TippingPoint Advanced Threat Protection Analyzer sets the user account to inactive (locked). You can unlock the account in the **Accounts** screen. **Tip** Record the user name and password for future reference.
Description	(Optional) Type a description that does not exceed 40 characters.
Role	Select the role and associated permissions of this user account. • **Administrator**: Users have full access to submitted objects, analysis results, and product settings • **Investigator**: Users have read-only access to submitted objects, analysis results, and product settings, but can download the investigation package, including submitted objects • **Operator**: Users have read-only access to submitted objects, analysis results, and product settings
Add to contacts	Select to add this user account to the **Contacts** list.
Email address	Type the email address of the account owner.
Phone number	(Optional) Type the phone number of the account owner.

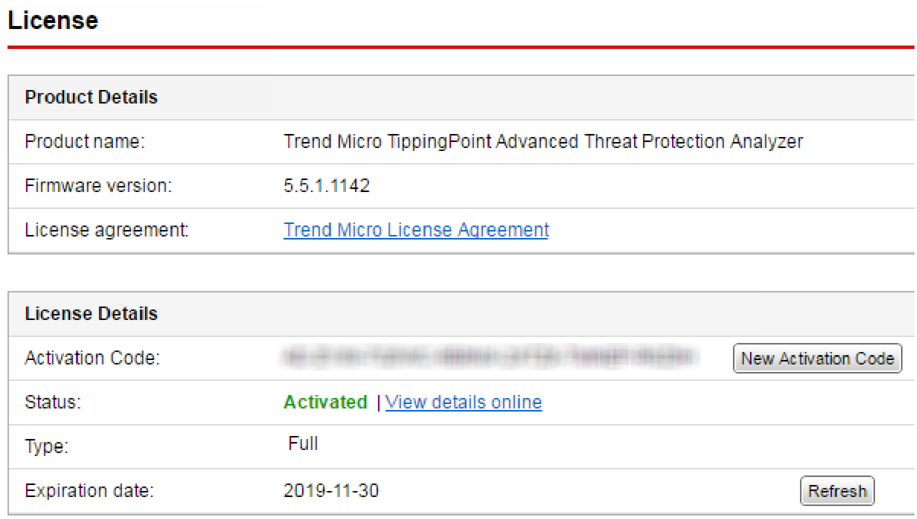
Getting Started Tasks

Procedure

1. Activate the product license using a valid Activation Code. For details, see *License on page A-8*.
2. Specify the TippingPoint Advanced Threat Protection Analyzer host name and IP address. For details, see *Network Tab on page A-11*.
3. Configure proxy settings if TippingPoint Advanced Threat Protection 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 TippingPoint Advanced Threat Protection Analyzer features operate as intended. For details, see *Time Tab on page A-14*.
5. Configure SMTP settings to enable sending of notifications through email. For details, see *SMTP Tab on page A-16*.
6. Import sandbox instances to Virtual Analyzer. For details, see *Importing an Image on page A-17*.
7. Configure Virtual Analyzer network settings to enable sandbox instances to connect to external destinations. For details, see *Enabling External Connections on page A-19*.
8. (Optional) Deploy and configure additional TippingPoint Advanced Threat Protection Analyzer appliances for use in a high availability or load-balancing cluster. For details, see *Cluster Tab on page A-20*.

License

Use the **License** screen, in **Administration** > **License**, to view, activate, and renew the TippingPoint Advanced Threat Protection Analyzer license.



License

Product Details	
Product name:	Trend Micro TippingPoint Advanced Threat Protection Analyzer
Firmware version:	5.5.1.1142
License agreement:	Trend Micro License Agreement

License Details	
Activation Code:	[redacted] New Activation Code
Status:	Activated | View details online
Type:	Full
Expiration date:	2019-11-30 Refresh

The TippingPoint Advanced Threat Protection 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:

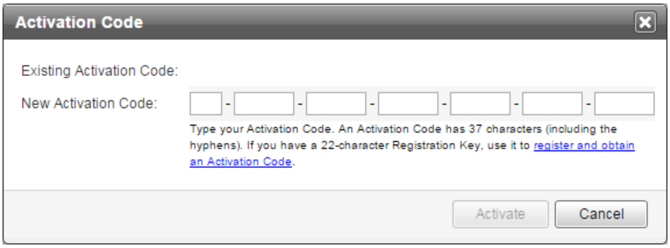
https://clp.trendmicro.com/fullregistration

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

TABLE A-4. Product Details

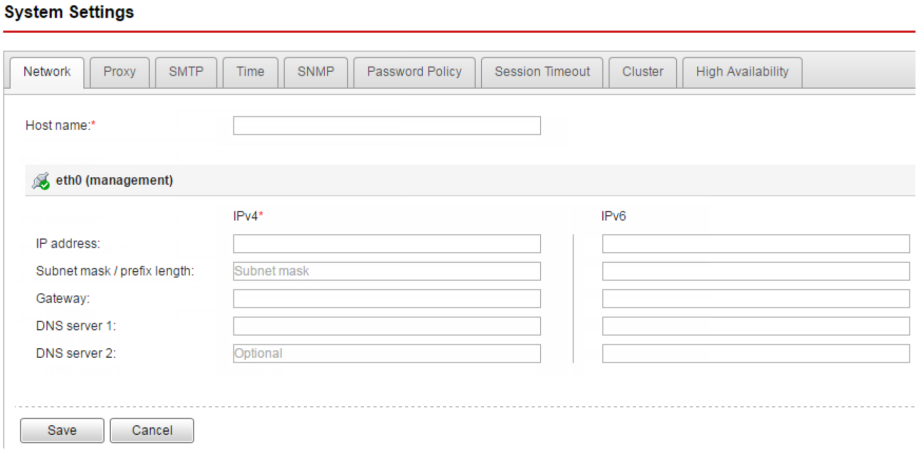
FIELD	DETAILS
Product name	Displays the name of the product.
Firmware version	Displays the full build number of the product.
License agreement	Displays a link to the **Trend Micro License Agreement**. Click the link to view or print the license agreement.

TABLE A-5. License Details

FIELD	DETAILS
Activation Code	View the Activation Code in this section. If your license has expired, obtain a new Activation Code from Trend Micro. To renew the license, click **New Activation Code**, and type the new Activation Code.  Activation Code Existing Activation Code: New Activation Code: Activate Cancel Type your Activation Code. An Activation Code has 37 characters (including the hyphens). If you have a 22-character Registration Key, use it to register and obtain an Activation Code. The **License** screen reappears displaying the number of days left before the product expires.
Status	Displays either **Activated**, **Not Activated**, **Evaluation**, or **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	• TippingPoint Advanced Threat Protection Analyzer: Provides access to all product features • TippingPoint Advanced Threat Protection Analyzer (Trial): Provides access to all product features
Expiration date	View the expiration date of the license. Renew the license before it expires.

Network Tab

Use this screen to configure the host name, the IPv4 and IPv6 addresses of the TippingPoint Advanced Threat Protection Analyzer appliance, and other network settings.



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*.

TippingPoint Advanced Threat Protection 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.

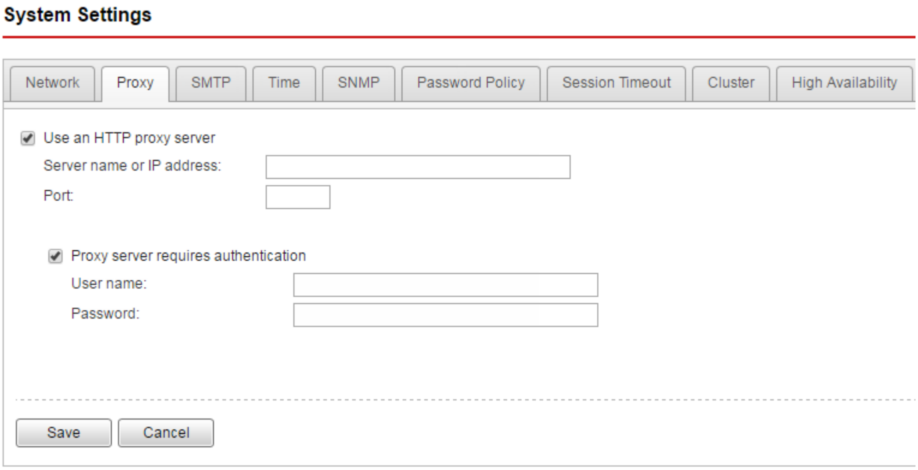
The following table lists configuration limitations.

Table A-6. Configuration Limitations

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

Proxy Tab

Specify proxy settings if TippingPoint Advanced Threat Protection Analyzer connects to the Internet or management network through a proxy server.


System Settings

☑ Use an HTTP proxy server

Server name or IP address:

Port:

☑ Proxy server requires authentication

User name:

Password:

Configure the following settings.

TABLE A-7. Proxy Tab Tasks

TASK	STEPS
Use an HTTP proxy server	Select this option to enable proxy settings.
Server name or IP address	Type the proxy server host name or IPv4 address, or IPv6 address. The management console does not support host names with double-byte encoded characters. If the host name includes such characters, type its IP address instead.
Port	Type the port number that TippingPoint Advanced Threat Protection Analyzer uses to connect to the proxy server.
Proxy server requires authentication	Select this option if the connection to the proxy server requires authentication. TippingPoint Advanced Threat Protection Analyzer supports the following authentication methods: • No authentication • Basic authentication • Digest authentication **Note** TippingPoint Advanced Threat Protection Analyzer product license cannot be validated when connecting to the Internet through proxy server with digest authentication. • NTMLv1 authentication
User name	Type the user name used for authentication. **Note** This option is only available if **Proxy server requires authentication** is enabled.

TASK	STEPS
Password	Type the password used for authentication. **Note** This option is only available if **Proxy server requires authentication** is enabled.

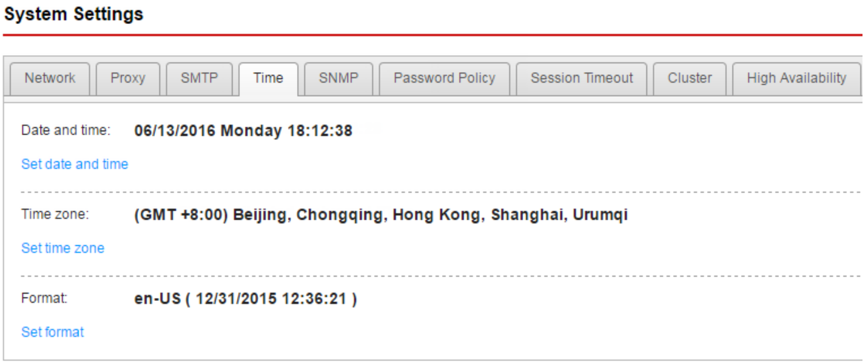
Time Tab

Configure date and time settings immediately after installation.

Procedure

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

   The **Time** screen appears.



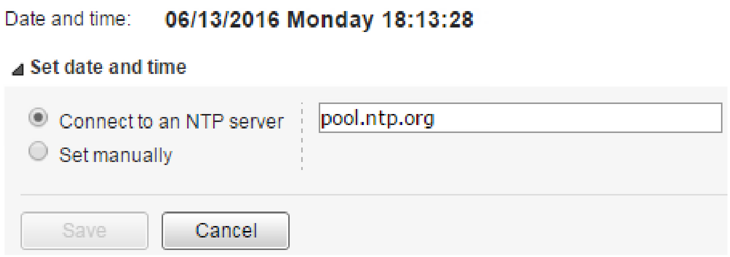
Date and time: 06/13/2016 Monday 18:12:38

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

Format: en-US (12/31/2015 12:36:21)

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

The settings panel appears.



Date and time: **06/13/2016 Monday 18:13:28**

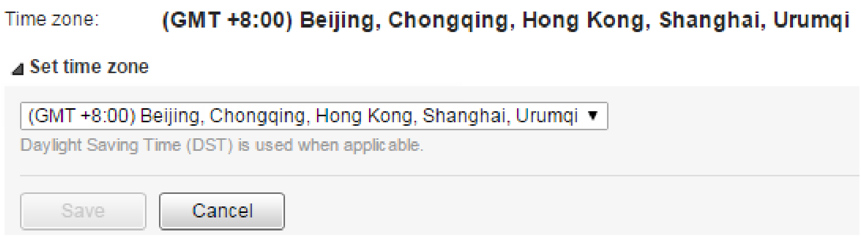
Set date and time

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

○ Set manually

3. Select one of the following methods and configure the applicable settings.
   - Select **Connect to an NTP server** and type the host name, IPv4 address, or IPv6 address of the NTP server.
   - Select **Set manually** and configure the time.
4. Click **Save**.
5. Click **Set time zone**.

   The settings panel appears.



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

Set time zone

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

Daylight Saving Time (DST) is used when applicable.

6. Select the applicable time zone.

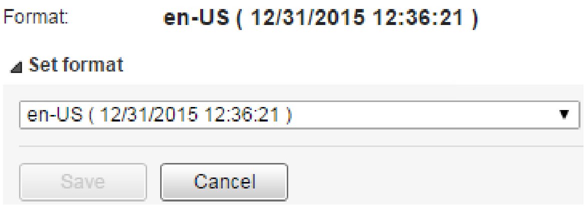
Note

Daylight Saving Time (DST) is used when applicable.

7. Click **Save**.

8. Click **Set format**.

   The settings panel appears.



Format: en-US (12/31/2015 12:36:21)

Set format

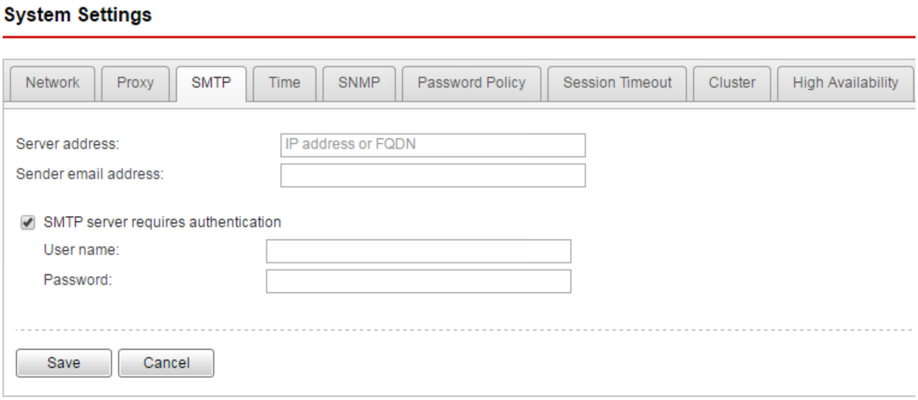
en-US (12/31/2015 12:36:21)

9. Select the preferred date and time format.

10. Click **Save**.

SMTP Tab

TippingPoint Advanced Threat Protection Analyzer uses SMTP settings when sending notifications through email.



System Settings

Server address: IP address or FQDN

Sender email address:

☑ SMTP server requires authentication

User name:

Password:

Configure the following settings.

TABLE A-8. SMTP Tab Tasks

TASK	STEPS
Server address	Type the SMTP server host name, IPv4 address, or IPv6 address. The management console does not support host names with double-byte encoded characters. If the host name includes such characters, type its IP address instead.
Sender email address	Type the email address of the sender.
SMTP server requires authentication	Select this option if connection to the SMTP server requires authentication.
User name	Type the user name used for authentication. **Note** This option is only available if **SMTP server requires authentication** is enabled.
Password	Type the password used for authentication. **Note** This option is only available if **SMTP server requires authentication** is enabled.

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.

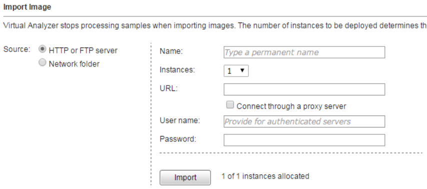
Procedure

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

   The **Images** screen appears.

2. Click **Import**.

   The **Import Image** screen appears.



Import Image

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

Source: ● HTTP or FTP server ○ Network folder

Name: *Type a permanent name*

Instances: 1 ▼

URL:

□ Connect through a proxy server

User name: *Provide for authenticated servers*

Password:

1 of 1 instances allocated

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

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

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

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

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

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

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

4. Click **Import**.

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

Note

If you selected **HTTP or FTP server**, TippingPoint Advanced Threat Protection 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.

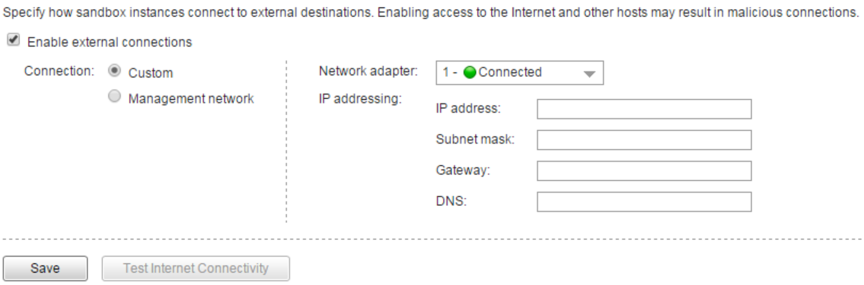
Procedure

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 ○ Management network

Network adapter: 1 - ● Connected

IP addressing:

IP address:

Subnet mask:

Gateway:

DNS:

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, such as a test network with Internet connection but without proxy settings, proxy authentication, and connection restrictions.

- 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. Click **Save**.

Cluster Tab

Multiple standalone TippingPoint Advanced Threat Protection 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 TippingPoint Advanced Threat Protection Analyzer appliances available, you may deploy the following cluster configurations:

TABLE A-9. Cluster Configurations

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

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

TABLE A-10. Cluster Configuration Modes

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

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

Configuration Mode	Description
Secondary	• Automatically configured based on the settings of the active primary appliance • Identifies the active primary appliance using its IP address or virtual IP address • Processes submissions allocated by the active primary appliance for performance improvement • Management console only shows screens with configurable settings: • **Virtual Analyzer** > **Sandbox Management** > **Network Connection** • **Virtual Analyzer** > **Sandbox Management** > **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** > **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

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

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

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

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

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

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

Note

- If your network has Trend Micro 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 *TippingPoint Advanced Threat Protection Analyzer Administrator's Guide*.

Update or upgrade the appliance firmware, hotfix, and patch version as necessary. For details, see the *TippingPoint Advanced Threat Protection 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 *TippingPoint Advanced Threat Protection Analyzer Administrator's Guide*.

c. Configure the appliance network settings.

For details, see *Network Tab on page A-11*.

d. Add accounts.

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

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-11*.

    Note

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

    Note

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

Index

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM57454/160713