TREND MICRO

5.5

# TREND MICRO™ TippingPoint™ Advanced Threat Protection Analyzer

## Administrator's 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

© 2016 Trend Micro Incorporated. All Rights Reserved.Trend Micro, the Trend Micro t-ball logo, and Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document Part No.: APEM57300/160118

Release Date: April 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 in the Trend Micro Online Help and/or the Trend Micro Knowledge Base at the Trend Micro website.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

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

# Table of Contents

## Preface


Preface ..... v

Documentation ..... vi

Audience ..... vii

Document Conventions ..... vii

Terminology ..... ix

About Trend Micro ..... xi


## Chapter 1: Introduction


About TippingPoint Advanced Threat Protection Analyzer ..... 1-2

What's New ..... 1-2

Features and Benefits ..... 1-3

- Enable Sandboxing as a Centralized Service ..... 1-4
- Custom Sandboxing ..... 1-4
- Broad File Analysis Range ..... 1-4
- YARA Rules ..... 1-4
- Document Exploit Detection ..... 1-5
- Automatic URL Analysis ..... 1-5
- Detailed Reporting ..... 1-5
- Alert Notifications ..... 1-5
- Clustered Deployment ..... 1-5
- Trend Micro Integration ..... 1-5
- Web Services API and Manual Submission ..... 1-6
- Custom Defense Integration ..... 1-6


## Chapter 2: Getting Started


The Preconfiguration Console ..... 2-2

The Management Console ..... 2-2

- Management Console Navigation ..... 2-4

Getting Started Tasks ..... 2-5

Integration with Trend Micro Products ..... 2-6
Sandbox Analysis ..... 2-6
Suspicious Objects List ..... 2-8
Exceptions ..... 2-10

## Chapter 3: Dashboard

Dashboard Overview ..... 3-2

Tabs ..... 3-3
Tab Tasks ..... 3-3
New Tab Window ..... 3-3

Widgets ..... 3-5
Widget Tasks ..... 3-5

Summary Tab ..... 3-8
Submissions Over Time ..... 3-9
Virtual Analyzer Summary ..... 3-10
Suspicious Objects ..... 3-11

System Status Tab ..... 3-11
Hardware Status ..... 3-12
Queued Samples ..... 3-13
Virtual Analyzer Status ..... 3-14

## Chapter 4: Virtual Analyzer

Virtual Analyzer ..... 4-2

Submissions ..... 4-2
Submissions Tasks ..... 4-9
Detailed Information Screen ..... 4-15
Investigation Package ..... 4-17

Suspicious Objects ..... 4-20
Suspicious Objects Tasks ..... 4-21

Exceptions ..... 4-23
Exceptions Tasks ..... 4-23

Sandbox Management ..... 4-25
Status Tab ..... 4-26
Images Tab ..... 4-28
YARA Rules tab ..... 4-31
Archive Passwords Tab ..... 4-35
Submission Settings Tab ..... 4-36
Network Connection Tab ..... 4-40
Smart Feedback Tab ..... 4-42
Cloud Sandbox Tab ..... 4-43

Submitters ..... 4-44

## Chapter 5: Alerts and Reports

Alerts ..... 5-2
Triggered Alerts Tab ..... 5-2
Rules Tab ..... 5-3

Reports ..... 5-25
Generated Reports Tab ..... 5-25
Schedules Tab ..... 5-28
Customization Tab ..... 5-32

## Chapter 6: Administration

Updates ..... 6-2
Components ..... 6-2
Component Update Settings Tab ..... 6-4
Hot Fixes / Patches Tab ..... 6-5
Firmware Tab ..... 6-9

System Settings ..... 6-11
Network Tab ..... 6-12
High Availability Tab ..... 6-13
Proxy Tab ..... 6-15
SMTP Tab ..... 6-17
Time Tab ..... 6-18
Password Policy Tab ..... 6-20
Session Timeout Tab ..... 6-21

Log Settings ..... 6-21
Configuring Syslog Settings ..... 6-22
Accounts / Contacts ..... 6-23
Accounts Tab ..... 6-24
Contacts Tab ..... 6-28
Audit Logs ..... 6-29
Querying Audit Logs ..... 6-30
System Maintenance ..... 6-30
Back Up Tab ..... 6-31
Restore Tab ..... 6-34
Power Off / Restart Tab ..... 6-35
Cluster Tab ..... 6-35
Tools ..... 6-49
Manual Submission Tool ..... 6-49
Image Preparation Tool ..... 6-51
License ..... 6-51
About TippingPoint Advanced Threat Protection Analyzer ..... 6-54

## Chapter 7: Technical Support

Troubleshooting Resources ..... 7-2
Contacting Trend Micro TippingPoint Support ..... 7-3
Sending Suspicious Content to Trend Micro ..... 7-4
Other Resources ..... 7-5

## Appendix A: Service Addresses and Ports

## Index

Index ..... IN-1

# Preface

## Preface

Welcome to the TippingPoint Advanced Threat Protection Analyzer *Administrator's Guide*. This guide contains information about product settings and service levels.

# 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.<br><br>The Administrator's Guide contains detailed instructions on how to configure and manage ATP Analyzer, and explanations on ATP Analyzer concepts and features. |
| Installation and Deployment Guide | PDF documentation provided with the product or downloadable from the Trend Micro website.<br><br>The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing 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.<br><br>The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in ATP Analyzer. |
| Quick Start Card | The Quick Start Card provides user-friendly instructions on connecting 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 ATP Analyzer management console.<br><br>The Online Help contains explanations of ATP Analyzer components and features, as well as procedures needed to configure 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:<br><br>http://esupport.trendmicro.com |

View and download product documentation from the Trend Micro Documentation 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<br>For example, **File** > **Save** means, click **File** and then click **Save** on the interface |
| **Note** | Configuration notes |
| **Tip** | Recommendations or suggestions |
| **Important** | Information regarding required or default configuration settings and product limitations |
| **WARNING!** | Critical actions and configuration options |

# Terminology

| Terminology | Description |
|---|---|
| ActiveUpdate | A component update source managed by Trend Micro. ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, program, and other Trend Micro component files through the Internet. |
| 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 | A cluster consists of at least two TippingPoint Advanced Threat Protection Analyzer appliances configured in a way that provides some sort of benefit.<br><br>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. |

| Terminology | Description |
|---|---|
| Management console | A web-based user interface for managing a product. |
| Management port | A hardware port that connects to the management network. |
| Passive primary appliance | Clustered appliance that is on standby until active primary appliance encounters an error and is unable to recover. Provides high availability. |
| Role-based administration | Role-based administration streamlines how administrators configure user accounts and control access to the management console. |
| 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 | A Trend Micro service that correlates suspicious objects detected in your environment and threat data from the Trend Micro Smart Protection Network. By providing on-demand access to Trend Micro intelligence databases, Threat Connect enables you to identify and investigate potential threats to your environment. |
| Virtual Analyzer | A secure virtual environment used to manage and analyze samples submitted by Trend Micro products. Sandbox images allow observation of file and network behavior in a natural setting. |
| Widget | A customizable screen to view targeted, selected data sets. |

| Terminology | Description |
| --- | --- |
| 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 Trend Micro™ TippingPoint Advanced Threat Protection Analyzer 5.5 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 TippingPoint Advanced Threat Protection products. The custom sandboxing environments that can be created within the 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**

| FEATURE/ENHANCEMENT | DETAILS |
|---|---|
| High availability | TippingPoint Advanced Threat Protection Analyzer provides the option of setting up a cluster environment to avoid having a single point of failure. |
| High-performance hardware | The TippingPoint Advanced Threat Protection Analyzer appliance allows a maximum of 60 sandbox instances. The hardware uses two 4TB hard disk drives that are configured in RAID1. |
| Automatic URL analysis | TippingPoint Advanced Threat Protection Analyzer now performs page scanning and sandbox analysis of URLs that are automatically submitted by integrating products. |
| System and application events notification | TippingPoint Advanced Threat Protection Analyzer provides immediate intelligence about system and application events through email notifications. |

| Feature/Enhancement | Details |
|---|---|
| Sample analysis prioritization | TippingPoint Advanced Threat Protection Analyzer provides the option of prioritizing objects for analysis. |
| Improved detection | TippingPoint Advanced Threat Protection Analyzer provides increased protection by improving its detection capabilities. The enhancements in this release include Office 2013 sandbox support, YARA rules support, unified VA analysis reports, and increased sandbox image support of up to 20GB. |
| Role-based administration | TippingPoint Advanced Threat Protection Analyzer now allows administrators to create and assign Investigator and Operator accounts. |
| Syslog server support for Trend Micro Event Format (TMEF) logs | TippingPoint Advanced Threat Protection Analyzer provides the option of sending logs to the syslog server in Trend Micro Event Format (TMEF). |
| Complete IPV4 and IPV6 dual-stack support | TippingPoint Advanced Threat Protection Analyzer supports IPV4 and IPV6 addresses for all settings. |
| Internet Explorer 11 and Edge browser support | TippingPoint Advanced Threat Protection Analyzer supports the latest versions of Internet Explorer. |
| Integration with Trend Micro products | TippingPoint Advanced Threat Protection Analyzer now allows integration with TippingPoint Advanced Threat Protection for Email and InterScan Web Security. |

# 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 for the TippingPoint Advanced Threat Protection and 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

# Getting Started

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

# 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.

For details, see the *TippingPoint Advanced Threat Protection Analyzer Installation and Deployment Guide*.

# 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:

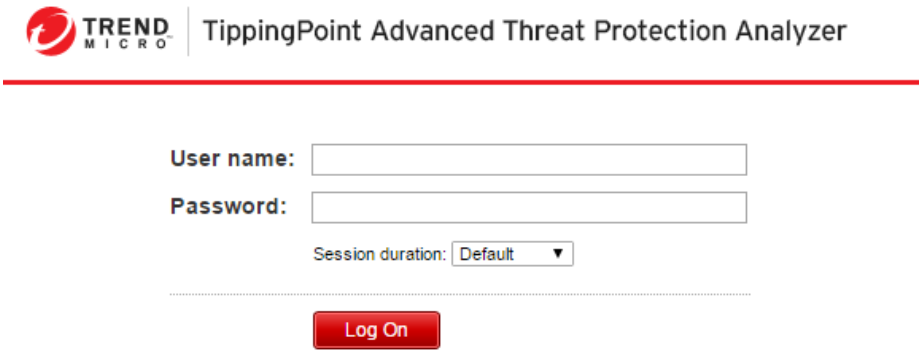



**TABLE 2-1. Management Console Logon Options**

| OPTION | DETAILS |
|---|---|
| User name | Type the logon credentials (user name and password) for the management console.<br><br>Use the default administrator logon credentials when logging on for the first time:<br><br>• User name: `admin`<br>• Password: `Admin1234!`<br><br>Trend Micro recommends changing the password after logging on to the management console for the first time.<br><br>Configure user accounts to allow other users to access the management console without using the administrator account. For details, see *Accounts Tab on page 6-24*. |
| Password | |

| Option | Details |
|---|---|
| Session duration | Choose how long you would like to be logged on.<br>• **Default**: 10 minutes<br>• **Extended**: 1 day<br>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. |

## Management Console Navigation

The management console consists of the following elements:

**Table 2-2. Management Console Elements**

| Section | Details |
|---|---|
| Banner | The management console banner contains:<br>• Product logo and name: Click to go to the dashboard. For details, see *Dashboard Overview on page 3-2*.<br>• Name of the user currently logged on to the management console.<br>• **Log Off** link: Click to end the current console session and return to the logon screen.<br>• System time: Displays the current system time and time zone. |
| Main Menu Bar | The main menu bar contains several menu items that allow you to configure product settings. For some menu items, such as **Dashboard**, clicking the item opens the corresponding screen. For other menu items, submenu items appear when you click or mouseover the menu item. Clicking a submenu item opens the corresponding screen. |

| Section | Details |
|---|---|
| Scroll Up and Arrow Buttons | Use the **Scroll up** option when a screen's content exceeds the available screen space. Next to the **Scroll up** button is an arrow button that expands or collapses the bar at the bottom of the screen. |
| Context-sensitive Help | Use **Help** to find more information about the screen that is currently displayed. |

# Getting Started Tasks

### Procedure

1. Activate the product license using a valid Activation Code. For details, see *License on page 6-51*.
2. Specify the TippingPoint Advanced Threat Protection Analyzer host name and IP address. For details, see *Network Tab on page 6-12*.
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 6-15*.
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 6-18*.
5. Configure SMTP settings to enable sending of notifications through email. For details, see *SMTP Tab on page 6-17*.
6. Import sandbox instances to Virtual Analyzer. For details, see *Importing an Image on page 4-29*.
7. Configure Virtual Analyzer network settings to enable sandbox instances to connect to external destinations. For details, see *Enabling External Connections on page 4-40*.

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 6-35*.

# Integration with Trend Micro Products

TippingPoint Advanced Threat Protection Analyzer integrates with the Trend Micro products listed in the following tables.

## Sandbox Analysis

Products that can send samples to TippingPoint Advanced Threat Protection Analyzer Virtual Analyzer for sandbox analysis:

**Note**

All samples display on the TippingPoint Advanced Threat Protection Analyzer management console, in the **Submissions** screen (**Virtual Analyzer** > **Submissions**). TippingPoint Advanced Threat Protection Analyzer administrators can also manually send samples from this screen.

| Product/Supported Versions | Integration Requirements and Tasks |
|---|---|
| TippingPoint Advanced Threat Protection for Email 2.5 or later | On the management console of the integrating product, go to the appropriate screen (see the product documentation for details on which screen to access) and specify the following information:<br>• API key. This is available on the TippingPoint Advanced Threat Protection Analyzer management console, in **Help** > **About**.<br>• TippingPoint Advanced Threat Protection Analyzer IP address. If unsure of the IP address, check the URL used to access the TippingPoint Advanced Threat Protection Analyzer management console. The IP address is part of the URL.<br>• TippingPoint Advanced Threat Protection Analyzer IPv4 or IPv6 virtual address. When using TippingPoint Advanced Threat Protection Analyzer in a high availability configuration, the virtual IP address is used to provide integrating products with a fixed IP address for configuration. This is available on the TippingPoint Advanced Threat Protection Analyzer management console, in **Administration** > **System Settings** > **High Availability**.<br>• TippingPoint Advanced Threat Protection Analyzer SSL port 443. This is not configurable.<br>**Important**<br>If the TippingPoint Advanced Threat Protection Analyzer API key changes after registering with the integrated product, remove TippingPoint Advanced Threat Protection Analyzer from the integrated product and add it again.<br>**Note**<br>Some integrating products require additional configuration to integrate with TippingPoint Advanced Threat Protection Analyzer properly. See the product documentation for details.<br>(Optional) On the TippingPoint Advanced Threat Protection Analyzer management console, review and modify the weight values of integrated products to adjust Virtual Analyzer resource allocation. For details see *Submitters on page 4-44*. |
| TippingPoint Advanced Threat Protection for Networks 3.7 or later | |
| ScanMail for Microsoft Exchange 11.0 or later | |
| ScanMail for IBM Domino 5.6 SP 1 Patch 1 HF4666 or later | |
| InterScan Messaging Security Virtual Appliance (IMSVA) 8.2 SP 2 or later | |
| InterScan Messaging Security Suite (IMSS) 7.5 or later | |
| InterScan Web Security Virtual Appliance (IWSVA) 6.0 or later | |
| InterScan Web Security Suite (IWSS) 6.5 | |
| Deep Edge 2.5 SP 2 or later | |

## Suspicious Objects List

Products that retrieve the suspicious objects list from TippingPoint Advanced Threat Protection Analyzer Virtual Analyzer:

| Product/Supported Versions | Integration Requirements and Tasks |
|---|---|
| TippingPoint Advanced Threat Protection for Networks 3.7 or later | On the management console of the integrating product, go to the appropriate screen (see the product documentation for information on which screen to access) and specify the following information:<br>• API key. This is available on the TippingPoint Advanced Threat Protection Analyzer management console, in **Help** > **About**.<br>• TippingPoint Advanced Threat Protection Analyzer IP address. If unsure of the IP address, check the URL used to access the TippingPoint Advanced Threat Protection Analyzer management console. The IP address is part of the URL.<br>• TippingPoint Advanced Threat Protection Analyzer IPv4 or IPv6 virtual address. When using TippingPoint Advanced Threat Protection Analyzer in a high availability configuration, the virtual IP address is used to provide integrated products with a fixed IP address for configuration. This is available on the TippingPoint Advanced Threat Protection Analyzer management console, in **Administration** > **System Settings** > **High Availability**.<br>• TippingPoint Advanced Threat Protection Analyzer SSL port 443. This is not configurable.<br>**Note**<br>Some of the integrating products require additional configuration to integrate with TippingPoint Advanced Threat Protection Analyzer properly. See the product documentation for details. |
| Standalone Smart Protection Server with the latest patch 2.6 or later | |
| OfficeScan Integrated Smart Protection Server 10.6 SP 2 Patch 1 to OfficeScan Integrated Smart Protection Server 11 SP 1 | |
| InterScan Web Security Virtual Appliance (IWSVA) 6.0 or later | |
| InterScan Web Security Suite (IWSS) 6.5 | |

| Product/Supported Versions | Integration Requirements and Tasks |
|---|---|
| Control Manager 6.0 SP 3 HF 3158 or later | On the management console of the integrating product, go to the appropriate screen (see the product documentation for information on which screen to access) and specify the following information:<br>• TippingPoint Advanced Threat Protection Analyzer IPv4 or IPv6 address. If unsure of the IP address, check the URL used to access the TippingPoint Advanced Threat Protection Analyzer management console. The IP address is part of the URL.<br>• TippingPoint Advanced Threat Protection Analyzer IPv4 or IPv6 virtual address. When using TippingPoint Advanced Threat Protection Analyzer in a high availability configuration, the virtual IP address is used to provide integrated products with a fixed IP address for configuration. This is available on the TippingPoint Advanced Threat Protection Analyzer management console, in **Administration** > **System Settings** > **High Availability**.<br>• TippingPoint Advanced Threat Protection Analyzer SSL port 443. This is not configurable.<br>• TippingPoint Advanced Threat Protection Analyzer user logon credentials. For details, see *Accounts Tab on page 6-24*.<br>**Important**<br>If the TippingPoint Advanced Threat Protection Analyzer API key changes after registering with the integrated product, remove TippingPoint Advanced Threat Protection Analyzer from the integrated product and add it again.<br>**Note**<br>Some integrating products require additional configuration to integrate with TippingPoint Advanced Threat Protection Analyzer properly. See the product documentation for details. |

## Exceptions

Products that send exceptions to TippingPoint Advanced Threat Protection Analyzer Virtual Analyzer:

| Product/Supported Versions | Integration Requirements and Tasks |
|---|---|
| Control Manager 6.0 SP 3 HF 3158 or later | On the management console of the integrating product, go to the appropriate screen (see the product documentation for information on which screen to access) and specify the following information:<br>• TippingPoint Advanced Threat Protection Analyzer IPv4 or IPv6 address. If unsure of the IP address, check the URL used to access the TippingPoint Advanced Threat Protection Analyzer management console. The IP address is part of the URL.<br>• TippingPoint Advanced Threat Protection Analyzer IPv4 or IPv6 virtual address. When using TippingPoint Advanced Threat Protection Analyzer in a high availability configuration, the virtual IP address is used to provide integrated products with a fixed IP address for configuration. This is available on the TippingPoint Advanced Threat Protection Analyzer management console, in **Administration** > **System Settings** > **High Availability**.<br>• TippingPoint Advanced Threat Protection Analyzer SSL port 443. This is not configurable.<br>• TippingPoint Advanced Threat Protection Analyzer user logon credentials. For details, see *Accounts Tab on page 6-24*.<br>**Important**<br>If the TippingPoint Advanced Threat Protection Analyzer API key changes after registering with the integrated product, then TippingPoint Advanced Threat Protection Analyzer will need to be deleted from the integrated product and added again.<br>**Note**<br>Some integrating products require additional configuration to integrate with TippingPoint Advanced Threat Protection Analyzer properly. See the product documentation for details. |

# Chapter 3

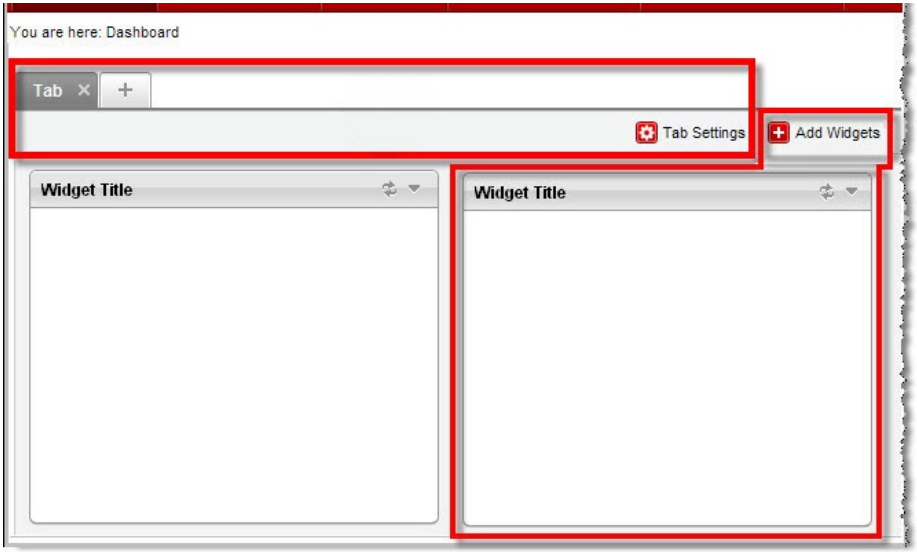
# Dashboard

This chapter describes the Trend Micro TippingPoint Advanced Threat Protection Analyzer dashboard.

# Dashboard Overview

Monitor your network integrity with the dashboard. Each management console user account has an independent dashboard. Any changes to a user account's dashboard does not affect other user accounts' dashboards.

The dashboard consists of the following user interface elements:




- Tabs provide a container for widgets. For details, see *Tabs on page 3-3*.
- Widgets represent the core dashboard components. For details, see *Widgets on page 3-5*.

---

Note

Click **Play Tab Slide Show** to show a dashboard slide show.

---

# Tabs

Tabs provide a container for widgets. Each tab on the dashboard can hold up to 20 widgets. The dashboard itself supports up to 30 tabs.

## Tab Tasks

The following table lists all the tab-related tasks:

| Task | Steps |
|---|---|
| Add a tab | Click the **plus** icon ( + ) on top of the dashboard. The **New Tab** window displays. For details, see *New Tab Window on page 3-3*. |
| Edit a tab's settings | Click **Tab Settings**. A window similar to the **New Tab** window opens, where you can edit settings. |
| Move a tab | Use drag-and-drop to change a tab's position. |
| Delete a tab | Click the **delete** icon ( ) next to the tab title. Deleting a tab also deletes all the widgets in the tab. |

## New Tab Window

The **New Tab** window opens when you add a new tab in the dashboard.

This window includes the following options:

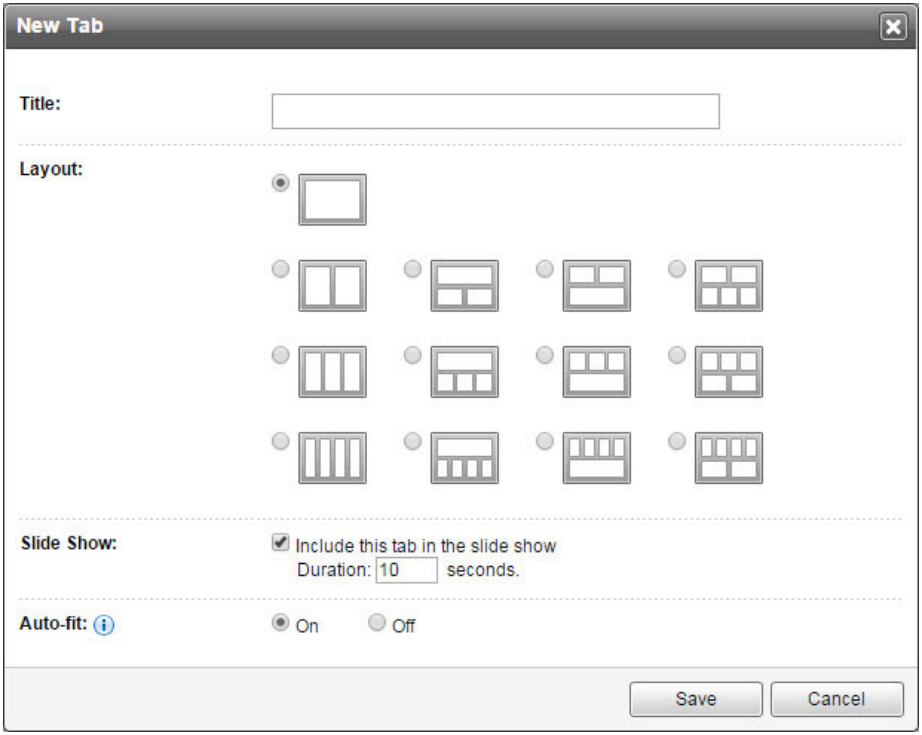



**TABLE 3-1. New Tab Options**

| TASK | STEPS |
|---|---|
| Title | Type the name of the tab. |
| Layout | Choose from the available layouts. |
| Slide Show | Select to include the tab in the Dashboard slide show. |
| Duration | Type the number of seconds to include the tab in the Dashboard slide show. |

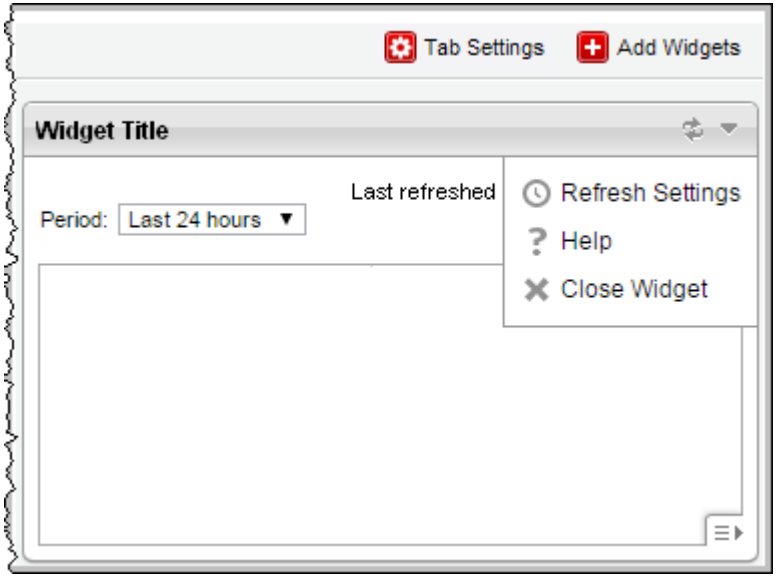
| Task | Steps |
|---|---|
| Auto-fit | Choose **On** or **Off**. This feature works when there is only one widget in a column. Choose **On** to adjust the height of the single widget to match the highest column. |

# Widgets

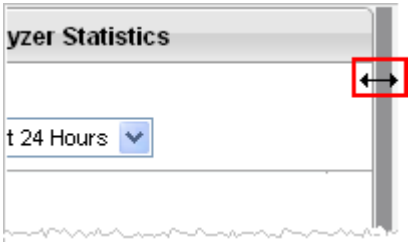
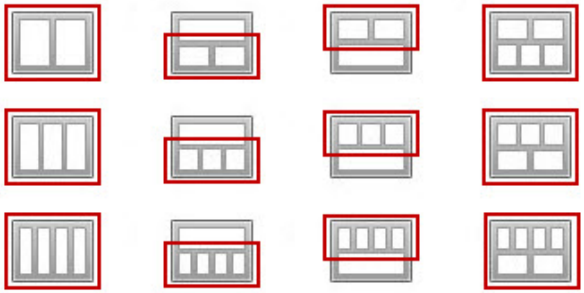
Widgets are the core components of the dashboard. Widgets contain charts and graphs that allow you to monitor the system status and track threats.

## Widget Tasks

The following table lists widget-related tasks:



| Task | Steps |
|---|---|
| Add a widget | Open a tab and then click **Add Widgets** at the top right corner of the tab. The Add Widgets screen displays. For details, see *Adding Widgets to the Dashboard on page 3-7*. |
| Refresh a widget's data | Click the refresh icon ( ). |
| Delete a widget | Click the arrow icon ( ) and then click **Close Widget**. This action removes the widget from the tab that contains it, but not from the other tabs that contain it or from the widget list in the **Add Widgets** screen. |
| Change the period | If available, click the **Period** drop-down box on top of the widget to change the time period. |
| Change the node | If available, click the **Node** drop-down box on top of the widget to change the node. |
| Move a widget | Use drag-and-drop to move a widget to a different location within the tab. |

| Task | Steps |
|---|---|
| Resize a widget | To resize a widget, point the cursor to the right edge of the widget. When you see a thick vertical line and an arrow (as shown in the following image), hold and then move the cursor to the left or right.<br>  <br><br>Only widgets on multi-column tabs are resizable. These tabs have any of the following layouts and the highlighted sections contain widgets that are resizable.<br>  |

## Adding Widgets to the Dashboard

The **Add Widgets** screen appears when you add widgets from a tab on the dashboard.

Do any of the following:

**Procedure**

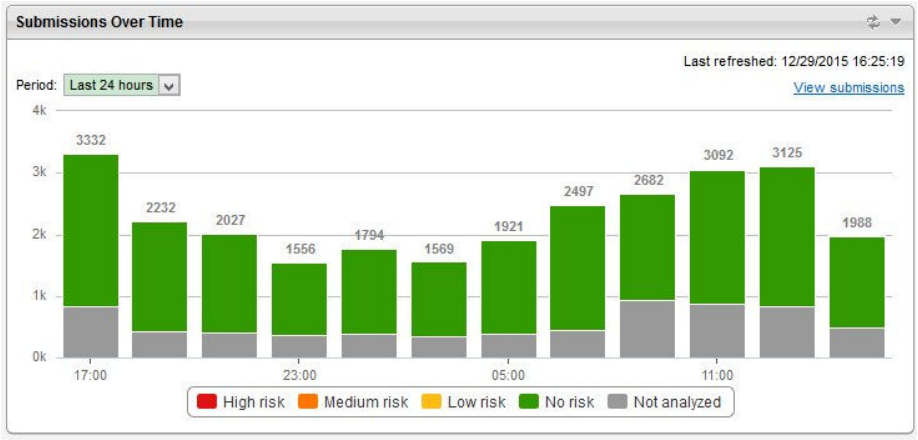
- To reduce the widgets that appear, click a category from the left side.
- To search for a widget, specify the widget name in the search text box at the top.
- To change the widget count per page, select a number from the **Records** drop-down menu.
- To switch between the Detailed and Summary views, click the display icons ( ) at the top right.
- To select the widget to add to the dashboard, select the check box next to the widget's title.
- To add the selected widgets, click **Add**.

# Summary Tab

View the **Summary** tab widgets to understand the types of threats detected by TippingPoint Advanced Threat Protection Analyzer based on submissions over time, the Virtual Analyzer summary, and the volume of suspicious objects discovered during analysis.

## Submissions Over Time

This widget plots the number of samples submitted to Virtual Analyzer over a period of time.



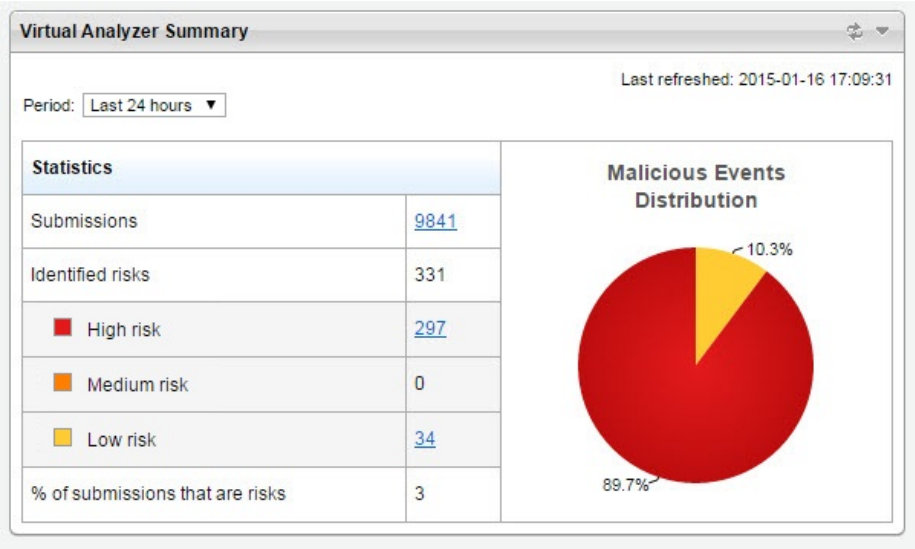

The default period is **Last 24 hours**. Change the period according to your preference.

Click **View submissions** to go to the **Submissions** screen and view detailed information.

For details, see *Submissions on page 4-2*.

## Virtual Analyzer Summary

This widget shows the total number of samples submitted to Virtual Analyzer and the number of these samples with risk.



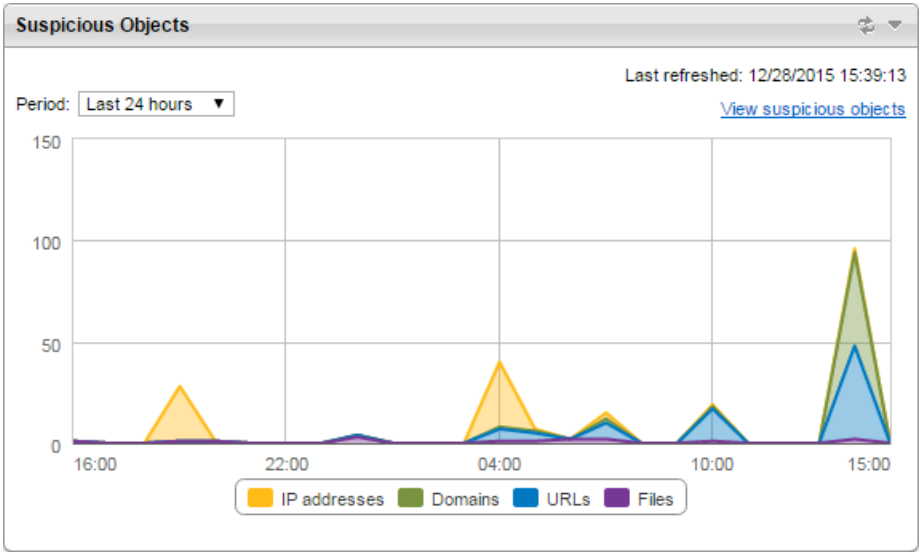

The default period is **Last 24 hours**. Change the period according to your preference.

Click the total number of submissions or the number of submissions with **High risk**, **Medium risk**, or **Low risk** to go to the **Submissions** screen and view detailed information.

For details, see *Submissions on page 4-2*.

## Suspicious Objects

This widget plots the number of objects (IP addresses, domains, URLs, and files) added to the Suspicious Objects list during the specified time period.




The default period is **Last 24 hours**. Change the period according to your preference.

Click **View suspicious objects** to go to the **Suspicious Objects** screen and view detailed information.

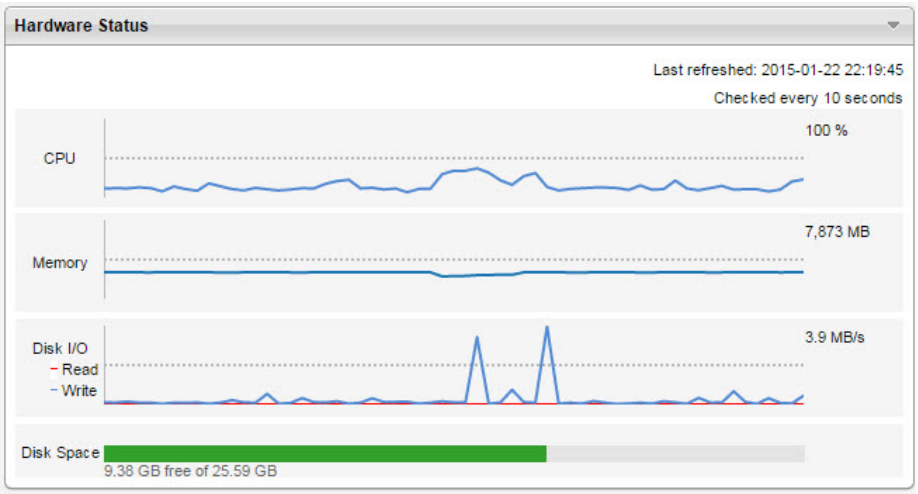
For details, see *Suspicious Objects on page 4-20*.

# System Status Tab

View the widgets in the **System Status** tab to understand the overall performance of TippingPoint Advanced Threat Protection Analyzer based on the hardware status, queued samples, and Virtual Analyzer status.

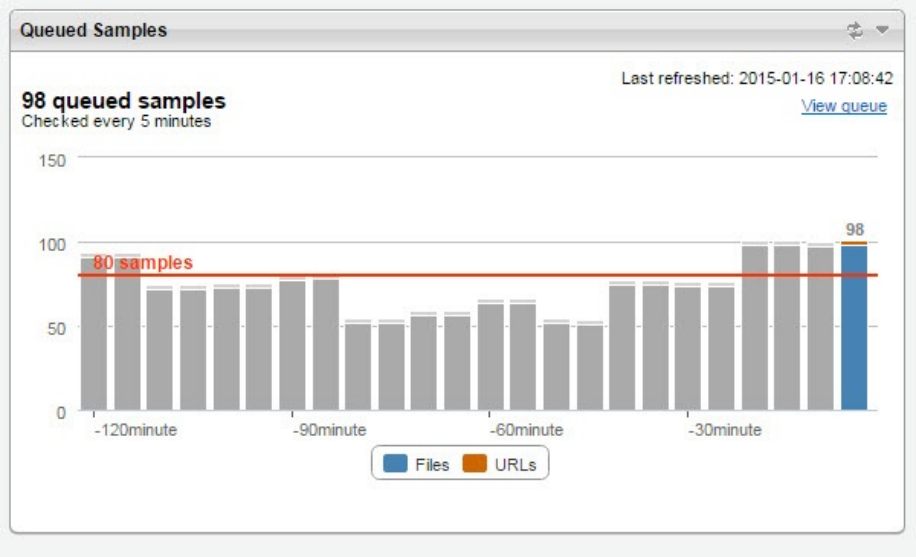
## Hardware Status

This widget displays the real-time utilization of key hardware components.



## Queued Samples

This widget displays the number of queued samples in Virtual Analyzer. The red line indicates the estimated number of samples Virtual Analyzer can analyze within 5 minutes.

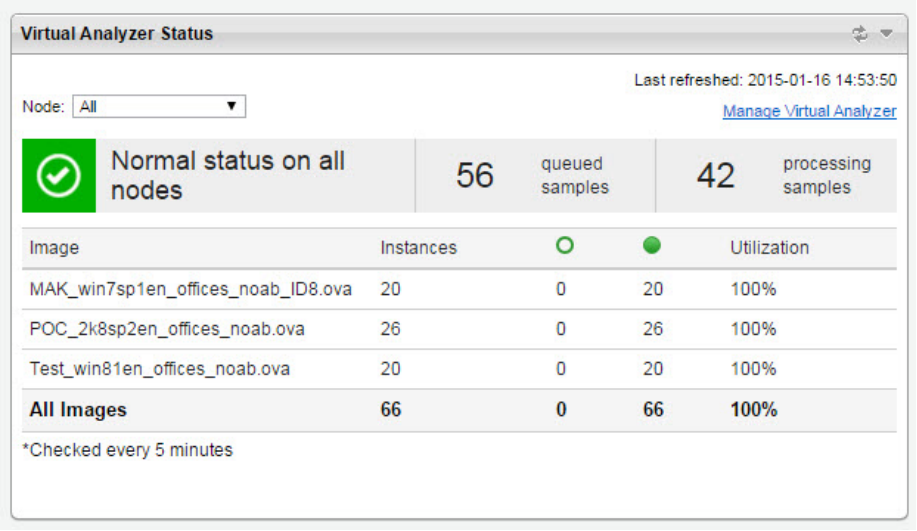



Click **View queue** to go to the **Queued** tab in the **Submissions** screen and view detailed information.

For details, see *Submissions on page 4-2*.

## Virtual Analyzer Status

This widget displays the status of Virtual Analyzer on one or all nodes. The widget content includes the number of queued and processing samples, and the number of instances for each image.




Click **Manage Virtual Analyzer** to go to the **Sandbox Management** screen. For details, see *Sandbox Management on page 4-25*.

**Normal status on all nodes** indicates all nodes are operating without errors.

If the status shows an error on one or more nodes, go to **Administration** > **System Maintenance** and click the **Cluster** tab to view detailed information about the error.

# Chapter 4

# Virtual Analyzer

This chapter describes the Virtual Analyzer.

# Virtual Analyzer

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products and administrators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.

Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics in the following categories:

- Anti-security and self-preservation
- Autostart or other system configuration
- Deception and social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformed, defective, or with known malware traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity

During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer also generates analysis reports, suspicious object lists, PCAP files, and OpenIOC files that can be used in investigations.

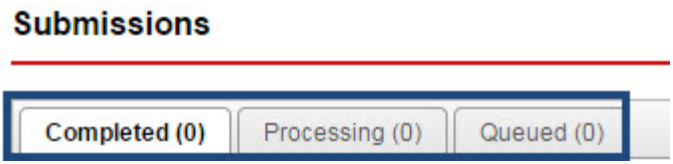
It works in conjunction with Threat Connect, the Trend Micro service that correlates suspicious objects detected in your environment and threat data from the Smart Protection Network.

# Submissions

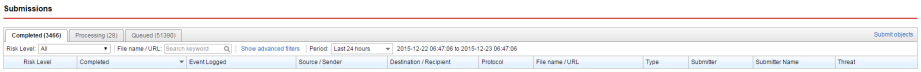
The **Submissions** screen, in **Virtual Analyzer** > **Submissions**, includes a list of samples processed by Virtual Analyzer. Samples are files and URLs submitted automatically by

Trend Micro products or manually by TippingPoint Advanced Threat Protection Analyzer administrators.

The **Submissions** screen organizes samples into the following tabs:




- **Completed**:
  - Samples that Virtual Analyzer has analyzed
  - Samples that have gone through the analysis process but do not have analysis results due to errors
- **Processing**: Samples that Virtual Analyzer is currently analyzing
- **Queued**: Samples that are pending analysis




On the tabs in the screen, check the following columns for basic information about the submitted samples:

**TABLE 4-1. Submissions Columns**

| COLUMN NAME AND TAB WHERE SHOWN | INFORMATION | |
|---|---|---|
| | FILE/EMAIL MESSAGE SAMPLE | URL SAMPLE |
| Risk Level<br><br>(**Completed** tab only) | Virtual Analyzer performs static analysis and behavior simulation to identify a sample's characteristics. During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the sample based on the accumulated ratings. | |

| Column Name and Tab Where Shown | Information | |
|---|---|---|
| | File/Email Message Sample | URL Sample |
| | • **Red icon** (🔴): High risk. The sample exhibited highly suspicious characteristics that are commonly associated with malware.<br>Examples:<br>• Detected as known malware<br>• Contains exploit code in document<br>• Attempts to connect to malicious host<br>• Stops or modifies antivirus service<br>• Downloads executable payload<br>• Hides file in system folder to evade detection<br>• Hides service using rootkit<br>• Exhibits behavior associated with ransomware<br>• **Orange icon** (🟠): Medium risk. The sample exhibited moderately suspicious characteristics that are also associated with benign applications.<br>• **Yellow icon** (🟡): Low risk. The sample exhibited mildly suspicious characteristics that are most likely benign.<br>• **Green icon** (🟢): No risk. The sample did not exhibit suspicious characteristics.<br>• **Gray icon** (⚪): Not analyzed.<br>For possible reasons why Virtual Analyzer did not analyze a file, see *Table 4-2: Possible Reasons for Analysis Failure on page 4-7*. | |

| Column Name and Tab Where Shown | Information | |
|---|---|---|
| | File/Email Message Sample | URL Sample |
| | **Note**<br>If a sample was processed by several instances, the icon for the most severe risk level displays. For example, if the risk level on one instance is yellow and then red on another instance, the red icon displays.<br>Mouseover the icon for details about the risk level. | |
| Completed<br>(**Completed** tab only) | Date and time that sample analysis was completed | |
| Event Logged<br>(All tabs) | • For samples submitted by other Trend Micro products, the date and time the product dispatched the sample<br>• For manually submitted samples, the date and time TippingPoint Advanced Threat Protection Analyzer received the sample | |
| Elapsed Time<br>(**Processing** tab only) | The amount of time that has passed since processing started | |
| Time in Queue<br>(**Queued** tab only) | The amount of time that has passed since Virtual Analyzer added the sample to the queue | |
| Source / Sender<br>(All tabs) | Where the sample originated<br>• IP address for network traffic or email address for email<br>• No data (indicated by a dash) if manually submitted | |
| Destination / Recipient<br>(All tabs) | Where the sample is sent<br>• IP address for network traffic or email address for email<br>• No data (indicated by a dash) if manually submitted | |
| Protocol | • Protocol used for sending the sample, such as SMTP for email or HTTP for network traffic | |

| Column Name and Tab Where Shown | Information | |
|---|---|---|
| | File/Email Message Sample | URL Sample |
| (**Completed** tab only) | • No data (indicated by a dash) if manually submitted | |
| File Name / URL<br><br>(**Completed** tab only) | • File name of the sample<br>• File name of the archive / File name of highest risk child object<br>• File name of the archive / File name of any child object if no risk<br><br>**Note**<br>"NONAMEFL" if file size is 0 or too small for analysis | URL<br><br>**Note**<br>TippingPoint Advanced Threat Protection Analyzer may have normalized the URL when submitted using the management console. |
| File Name / Email Subject / URL<br><br>(**Processing** and **Queued** tabs) | File name or email subject of the sample | URL<br><br>**Note**<br>TippingPoint Advanced Threat Protection Analyzer may have normalized the URL when submitted using the management console. |
| Type<br><br>(**Completed** tab only) | • Type of the object<br>• Type of the archive / Type of the highest risk child object<br>• Type of the archive / Type of any child object if no risk | • URL<br>• URL / Type of the object |

| Column Name and Tab Where Shown | Information | |
|---|---|---|
| | File/Email Message Sample | URL Sample |
| | **Note**<br>"Empty" or "UNKNOWN" if file size is 0 or too small to identify file type for analysis | |
| Submitter<br>(All tabs) | • Name of the Trend Micro product that submitted the sample<br>• "Manual Submission" if manually submitted | |
| Submitter Name<br>(All tabs) | • Host name of the Trend Micro product that submitted the sample<br>• No data (indicated by a dash) if manually submitted | |
| Threat<br>(**Completed** tab only) | Name of threat as detected by Trend Micro pattern files and other components | |

If the Risk Level column generates a gray icon (●), Virtual Analyzer has not analyzed the sample. The following table lists possible reasons for analysis failure and identifies actions you can take.

**Table 4-2. Possible Reasons for Analysis Failure**

| Reason | Action |
|---|---|
| Unsupported file type | To request a list of supported file types, contact Trend Micro support.<br><br>**Note**<br>If a file has multiple layers of encrypted compression (for example, encrypted compressed files within a compressed file), Virtual Analyzer is unable to analyze the file, and displays the "Unsupported File Type" error. |

| Reason | Action |
|---|---|
| Microsoft Office 2007/2010 not installed on the sandbox image | Verify that Microsoft Office 2007 or 2010 has been installed on the sandbox by going to **Virtual Analyzer** > **Sandbox Management**. For details, see *Sandbox Management on page 4-25*. |
| Unable to simulate sample on the operating system | Verify that TippingPoint Advanced Threat Protection Analyzer supports the operating system installed on the sandbox image. |
| Unable to extract archive content using the user-defined password list | Check the password list in **Virtual Analyzer** > **Sandbox Management** > **Archive Passwords** tab. |
| URL character limit exceeded | Verify that the URL does not exceed 2,048 characters. |
| File size limit exceeded | Verify that the file size does not exceed 60MB. |
| Unsupported encryption or compression format | Decrypt or extract the file and resubmit the object for analysis. |
| Unable to access the Internet | Verify that external connections are enabled. |
| Unable to connect to the cloud sandbox | Verify the connection of the management network to the Internet. |
| Cloud sandbox analysis timed out | Resubmit the object for analysis. If the issue persists, contact your support provider. |
| Internal error occurred on the cloud sandbox | Please contact your support provider. |
| Internal error (with error number) occurred | Please contact your support provider. |

## Submissions Tasks

The following table lists all the **Submissions** tasks:

**TABLE 4-3. Submissions Tasks**

| TASK | STEPS |
|---|---|
| Submit Objects | Click **Submit** when you are done and then check the status in the **Processing** or **Queued** tab. When the sample has been analyzed, it appears in the **Completed** tab.<br><br>For details, see *Submitting Objects on page 4-12*.<br><br>To manually submit multiple files at once, use the Manual Submission Tool. See *Manually Submitting Objects on page 4-14*. |
| Detailed Information Screen | On the **Completed** tab, click anywhere on a row to view detailed information about the submitted sample. A new section below the row shows the details.<br><br>For details, see *Detailed Information Screen on page 4-15*. |
| Prioritize Objects | On the **Queued** tab, select an object and click **Prioritize** to move the object to the top of the queue. |

| TASK | STEPS |
|---|---|
| Data Filters | If there are too many entries in the table, limit the entries by performing any of these tasks:<br> <br><br>• Select a risk level in the **Risk level** drop-down box.<br>• On the **Completed** tab, type some characters in the **Search keyword** text box next to **File name/URL**, and then press ENTER. TippingPoint Advanced Threat Protection Analyzer searches only the file names, child file names, and URLs in the table for matches.<br>• On the **Processing** and **Queued** tabs, type some characters in the **Search keyword** text box next to **File name/Email subject/URL**, and then press ENTER. TippingPoint Advanced Threat Protection Analyzer searches only the file names, email subjects, and URLs in the table for matches.<br>• The **Period** drop-down box limits the entries according to the specified time period. If no time period is selected, the default configuration of **Last 24 hours** is used. This information only appears on the **Completed** tab.<br>All time periods indicate the time used by TippingPoint Advanced Threat Protection Analyzer.<br>• The **Show advanced filters** link can limit the entries according to information specified in one or more columns. For details, see *Applying Advanced Filters on page 4-10*. |
| Records and Pagination Controls | The panel at the bottom of the screen shows the total number of samples. If all samples cannot display at the same time, use the pagination controls to view the samples that are hidden from view. |

## Applying Advanced Filters

### Procedure

1. Click **Show advanced filters**.

The submission filters appear.

Message ID: Separate each item with a semicolon (;)

SHA-1 hash value: Separate each item with a semicolon (;)

Type:

Email subject:

Threat:

Submitter: Any

Submitter name:

Protocol:

Source / Sender:

Destination / Recipient:

Clear Apply Cancel

2. Type the information to filter into the text boxes.

**Note**

The **Completed** and **Queued** tabs contain fewer submission filters because analysis has not been completed.

- **Message ID**
- **SHA-1 hash value**
- **Type**

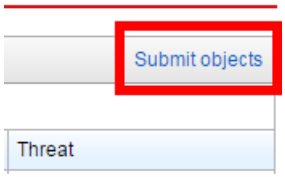
- Email subject
- Threat
- Submitter name
- Protocol
- Source / Sender
- Destination / Recipient

3. In the **Submitter** drop-down box, select a submitter to filter only objects from that submitter.
4. Click **Apply**.

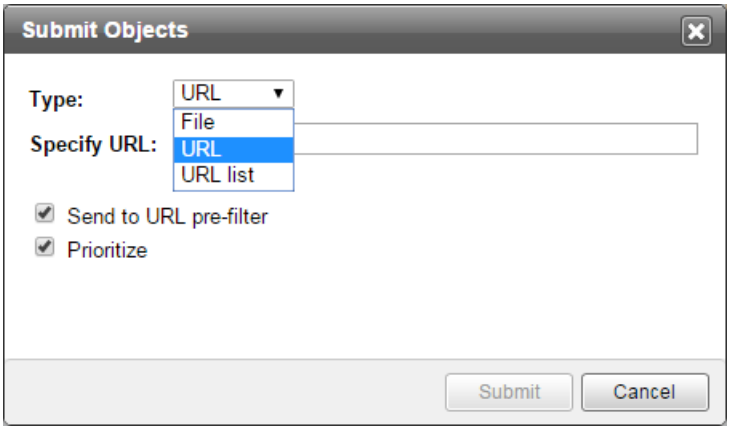
## Submitting Objects

**Procedure**

1. Go to **Virtual Analyzer** > **Submissions**.
2. Click **Submit Objects**.



The **Submit objects** window appears.




3. Select an object type:

| Type | Details and Instructions |
|---|---|
| File | Browse and select the sample. |
| Single URL | Type the URL in the text box provided. |
| URL list | Prepare a TXT or CSV file with a list of URLs (HTTP or HTTPS) in the first column of the file. When the file is ready, drag-and-drop the file in the **Select file** field or browse and select the file. |

4. (Optional) Select the following:

   - **Send to URL pre-filter**: Send submitted URLs to the URL pre-filter. URLs found safe by the URL pre-filter will not be sent to Virtual Analyzer for scanning and analysis.
   - **Prioritize**: Put submitted objects at the top of the queue.

5. Click **Submit**.

**Note**

To manually submit multiple files at once, use the Manual Submission Tool. For details, see *Manually Submitting Objects on page 4-14*.

## Manually Submitting Objects

### Procedure

1. If it is not already installed, install the Manual Submission Tool. For details, see *Manual Submission Tool on page 6-49*.
2. Go to the Manual Submission Tool package folder, open the `work` folder, and then place all of the sample files or an URL list file into the `indir` folder.
3. Run `cmd.exe`, and change the directory (`cd`) to the tool package folder.
4. Depending on the type of object you want to upload, do one of the following:

**Tip**

Execute `dtascli.exe` for help.

- **File**: Execute `dtascli.exe -u` to upload all of the files in the `work/indor` folder to Virtual Analyzer.

  After executing `dtascli.exe -u`, `cmd.exe` shows the following, along with all of the files that were uploaded from the `work/indir` folder.

```
c:\submission_v1.2.1005>dtascli.exe -u
2016-01-27 15:39:04.390 INFO    **** welcome to use submission tool v1.2.1005 **
**
2016-01-27 15:39:04.391 INFO    indir: c:\submission_v1.2.1005\work\indir
2016-01-27 15:39:04.392 INFO    outdir: c:\submission_v1.2.1005\work\outdir
2016-01-27 15:39:04.394 INFO    Server:
2016-01-27 15:39:04.395 INFO    API Key:
2016-01-27 15:39:05.023 INFO    Register is success
2016-01-27 15:39:05.375 INFO    Unregister is success
```

- **URL list**: Execute `dtascli.exe -u --url` to upload the file `url.txt` in the `work/indir` folder to Virtual Analyzer.

After executing `dtascli.exe -u`, `cmd.exe` shows the following, along with all of the files that were uploaded from the `work/indir` folder.

```
c:\submission_v1.2.1005>dtascli.exe -u --url
2016-01-27 15:38:27,073 INFO     **** welcome to use submission tool v1.2.1005 **
**
2016-01-27 15:38:27,075 INFO     indir: c:\submission_v1.2.1005\work\indir
2016-01-27 15:38:27,078 INFO     outdir: c:\submission_v1.2.1005\work\outdir
2016-01-27 15:38:27,078 INFO     Server: [redacted]
2016-01-27 15:38:27,081 INFO     API Key: [redacted]
2016-01-27 15:38:27,750 INFO     Register is success
2016-01-27 15:38:27,937 INFO     Find URL sample: ahsgd
2016-01-27 15:38:28,555 INFO     Find URL sample: ahsd
2016-01-27 15:38:29,312 INFO     Unregister is success
```

5. After uploading the files to Virtual Analyzer, confirm that they are being analyzed in the management console. Click **Virtual Analyzer** > **Submissions** to locate the files.

   Shortly after submitting the files, before they have been analyzed, they appear in the **Processing** or **Queued** tab. When the samples have been analyzed, they appear in the **Completed** tab.

## Detailed Information Screen

On the **Completed** tab, click anywhere on a row to view detailed information about the submitted sample. A new section below the row shows the details.

The following fields are displayed on this screen:

| Field Name | Information | |
|---|---|---|
| | File/Email Message Sample | URL Sample |
| Submission details | • Basic data fields (such as Logged and File name) extracted from the raw logs<br>• Sample ID (SHA-1)<br>• Child files, if available, contained in or generated from the submitted sample<br>• The **Raw Logs** link shows all the data fields in the raw logs | • The following is a preview of the fields:<br> <br>Logged: Tue, 25 Jun 2013 06:09:36 +0000<br>URL: http://xvideos.com:80/<br>Sample ID (SHA-1): 6B3F17CD086487DDD120F8AA86782A90A00FFB9C<br>MD5: 70A7F6A5475B9E301E4F39A0E4F83FF1<br>File name: http://xvideos.com:80/<br>Raw Logs<br>• URL<br>**Note**<br>TippingPoint Advanced Threat Protection Analyzer may have normalized the URL. |
| Notable characteristics | • The categories of notable characteristics that the sample exhibits, which can be any or all of the following:<br>  • Anti-security, self-preservation<br>  • Autostart or other system reconfiguration<br>  • Deception, social engineering<br>  • File drop, download, sharing, or replication<br>  • Hijack, redirection, or data theft<br>  • Malformed, defective, or with known malware traits<br>  • Process, service, or memory object change<br>  • Rootkit, cloaking<br>  • Suspicious network or messaging activity<br>  • Other notable characteristic<br>• A number link that, when opened, shows the actual notable characteristics | |

| Field Name | Information | |
|---|---|---|
| | File/Email Message Sample | URL Sample |
| Other submission logs | A table that shows the following information about other log submissions:<br>• Logged<br>• Protocol<br>• Direction<br>• Source IP<br>• Source Host Name<br>• Destination IP<br>• Destination Host Name | |
| Reports | The PDF icon ( ) links to a downloadable PDF report and the HTML icon ( ) links to an interactive HTML report.<br>**Note**<br>An unclickable link means there were errors during simulation. Mouseover the link to view details about the error. | |
| Investigation package | **Download** links to a password-protected investigation package that you can download to perform additional investigations.<br>For details, see *Investigation Package on page 4-17*. | |
| Global intelligence | **View in Threat Connect** is a link that opens Trend Micro Threat Connect<br>The page contains detailed information about the sample. | |

## Investigation Package

The investigation package helps administrators and investigators inspect and interpret threat data generated from samples analyzed by Virtual Analyzer. It includes files in OpenIOC format that describe Indicators of Compromise (IOC) identified on the affected host or network.

The table below describes some of the files within the investigation package that will aid in an investigation.

**TABLE 4-4. Investigation Package Contents**

| PATH WITHIN THE INVESTIGATION PACKAGE | DESCRIPTION |
|---|---|
| `\%SHA1%` | Each folder at the root level, with an SHA-1 hash value as its name, is associated with one object. More than one folder of this type will only exist if the first object is an archive file or an email message. |
| `\%SHA1%\%imageID%` | Associated with a sandbox image that analyzed the object. |
| `\%SHA1%\%imageID%\drop\droplist` | Contains a list of the files that were generated or modified during analysis. |
| `\%SHA1%\%imageID%\memory\image.bin` | Contains the raw memory dump after the process was launched into memory. |
| `\%SHA1%\%imageID%\pcap\%SHA1%.pcap` | Contains captured network data that can be used to extract payloads. The file does not exist If no network data was generated. |
| `\%SHA1%\%imageID%\report\report.xml` | Contains the final analysis report for a single object for a specific image. |
| `\%SHA1%\%imageID%\report \blacklist.xml` | Contains a list of all suspicious objects detected during analysis. This file is empty if no suspicious objects were detected during analysis. |
| `\%SHA1%\%imageID%\report \openioc.ioc` | Contains technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise. |
| `\%SHA1%\%imageID%\screenshot\ %SHA1%-%N%.png` | A screenshot of a UI event that occurred during analysis. The file does not exist if no UI events occurred during analysis. |
| `\common` | Contains files that are common amongst all of the samples. |

| Path within the Investigation Package | Description |
|---|---|
| `\common\drop\%SHA1%` | Generated or modified during analysis. |
| `\common\sample\%SHA1%` | The submitted sample. |
| `\common\sample\extracted\%SHA1%` | Extracted from the sample during analysis. |
| `\%SHA1%.report.xml` | The final analysis report for all objects. |

## Investigation Package Data Retention

TippingPoint Advanced Threat Protection Analyzer can retain the investigation package data for up to 100 days, but the time can be reduced due to storage limitations.

**Note**

To ensure the availability of the investigation package data, Trend Micro recommends backing up the data to an external server. For details, see *Data Backup on page 6-32*.

The following examples illustrate how storage limitations can affect the amount of time that the investigation package data is retained in TippingPoint Advanced Threat Protection Analyzer.

Based on testing done by Trend Micro, the average size of the investigation package data is 8 MB. If TippingPoint Advanced Threat Protection Analyzer analyzes 8000 samples per day, then the resulting investigation package data is 64000 MB.

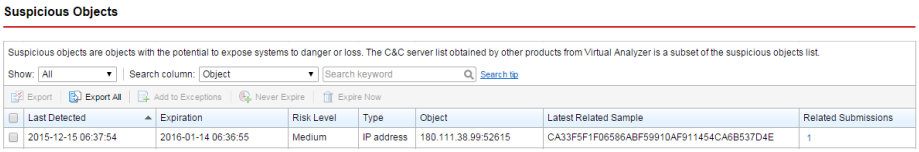
After about 62 days, the 4 TB disk from TippingPoint Advanced Threat Protection Analyzer 1100 is filled and the investigation package data is purged.

If TippingPoint Advanced Threat Protection Analyzer is in cluster mode, the disk space occupied per day is multiplied by the number of appliances in the cluster.

Using the numbers from the example above, the investigation package data for a cluster with five TippingPoint Advanced Threat Protection Analyzer 1100 appliances is purged after about 12 days.

# Suspicious Objects

Suspicious objects are objects with the potential to expose systems to danger or loss. TippingPoint Advanced Threat Protection Analyzer detects and analyzes suspicious IP addresses, host names, files, and URLs.




The following columns show information about objects added to the Suspicious Objects list:

**TABLE 4-5. Suspicious Objects Columns**

| COLUMN NAME | INFORMATION |
|---|---|
| Last Detected | Date and time Virtual Analyzer last found the object in a submitted sample |
| Expiration | Date and time Virtual Analyzer will remove the object from the **Suspicious Objects** tab |

| Column Name | Information |
|---|---|
| Risk Level | If the suspicious object is:<br>• **IP address** or **domain**: The risk level that typically shows is either **High** or **Medium** (see risk level descriptions below). This means that high- and medium-risk IP addresses/ domains are treated as suspicious objects.<br>**Note**<br>An IP address or domain with the **Low** risk level is also displayed if it is associated with other potentially malicious activities, such as accessing suspicious host domains.<br>• **URL**: The risk level that shows is **High**, **Medium**, or **Low**<br>• **File**: The risk level that shows is always **High**<br>Risk level descriptions:<br>• **High**: Known malicious or involved in high-risk connections<br>• **Medium**: IP address/domain/URL is unknown to reputation service<br>• **Low**: Reputation service indicates previous compromise or spam involvement |
| Type | **IP address**, **Domain**, **URL**, or **File** |
| Object | The IP address, domain, URL, or SHA-1 hash value of the file |
| Latest Related Sample | SHA-1 hash value of the sample where the object was last found. |
| Related Submissions | The total number of samples where the object was found.<br>Clicking the number opens the **Submissions** screen with the SHA-1 hash value as the search criteria. |

## Suspicious Objects Tasks

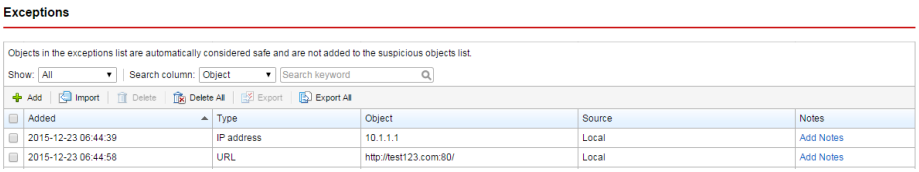
The following table lists all the **Suspicious Objects** tab tasks:

**TABLE 4-6. Suspicious Objects Tasks**

| TASK | STEPS |
|---|---|
| Export/Export All | Select one or several objects and then click **Export** to save the objects to a CSV file.<br><br>Click **Export All** to save all the objects to a CSV file. |
| Add to Exceptions | Select one or several objects that you consider harmless and then click **Add to Exceptions**. The objects move to the **Exceptions** tab. |
| Never Expire | Select one or several objects that you always want flagged as suspicious and then click **Never Expire**. |
| Expire Now | Select one or several objects that you want to remove from the **Suspicious Objects** and then click **Expire Now**. When the same object is detected in the future, it will be added back to the **Suspicious Objects**. |
| Data Filters | If there are too many entries in the table, limit the entries by performing these tasks:<br><br>• Select an object type in the **Show** drop-down box.<br><br>• Select a column name in the **Search column** drop-down box and then type some characters in the **Search keyword** text box next to it. As you type, the entries that match the characters you typed are displayed. TippingPoint Advanced Threat Protection Analyzer searches only the selected column in the table for matches. |
| Records and Pagination Controls | The panel at the bottom of the screen shows the total number of objects. If all objects cannot be displayed at the same time, use the pagination controls to view the objects that are hidden from view. |

# Exceptions

Objects in the exceptions list are automatically considered safe and are not added to the suspicious objects list. Manually add trustworthy objects or go to the **Virtual Analyzer** > **Suspicious Objects** screen and select suspicious objects that you consider harmless.




The following columns show information about objects in the exception list.

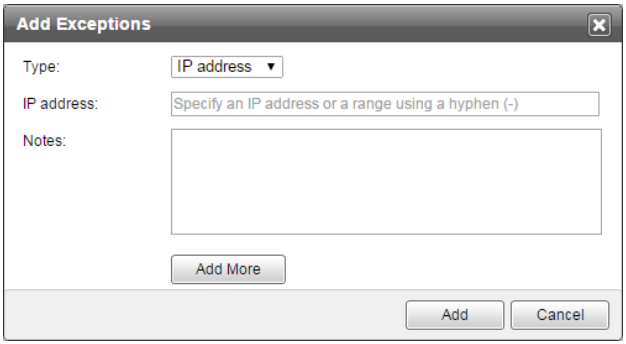
**TABLE 4-7. Exceptions Columns**

| COLUMN NAME | INFORMATION |
|---|---|
| Added | Date and time Virtual Analyzer added the object to the **Exceptions** tab |
| Type | IP address, domain, URL, or file |
| Object | The IP address, domain, URL, or SHA-1 hash value of the file |
| Source | The source (local or Control Manager) that added the exception |
| Notes | Notes for the object.<br>Click the link to edit the notes. |

## Exceptions Tasks

The following table lists all the **Exceptions** tab tasks:

**TABLE 4-8. Exceptions Tasks**

| TASK | STEPS |
|---|---|
| Add | 1. Click **Add** to add an object.<br>The **Add Exceptions** window appears.<br>  <br><br>2. Specify the **IP address**, **Domain**, **URL**, or **File** exception criteria.<br>• For IP addresses, select **IP address** for the type and then type the IP address or a hyphenated range.<br>• For domains, select **Domain** for the type and then type the domain.<br>**Note**<br>Wildcards are only allowed in a prefix. When a wildcard is used in a prefix, it must be connected with ". ". Only one wildcard may be used in a domain. For example, *.com will match abc.com or test.com.<br>• For URLs, select **URL** for the type and then type the URL.<br>**Note**<br>• Wildcards are only allowed in a prefix. When a wildcard is used in the domain part of an URL, it must be connected with ". ". Only one wildcard may be used in a URL. For example, http://*.com will match abc.com or test.com.<br>• When an unassigned wildcard is used in the URI part of an URL, it can match all parts. For example, http://abc.com/*abc will match http://abcd.com/test.abc. |

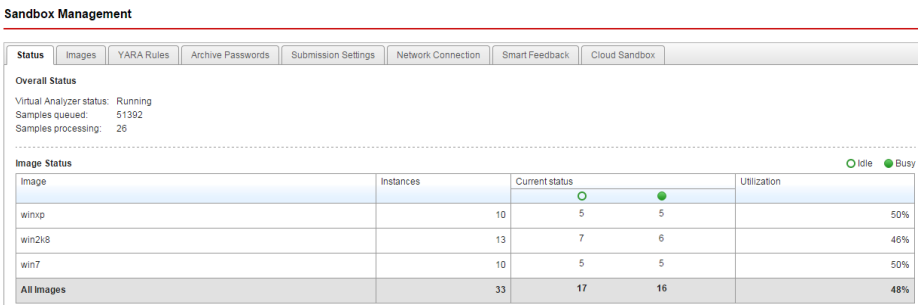
| Task | Steps |
|---|---|
| Import | Click **Import** to add objects from a properly-formatted CSV file. In the new window that opens:<br>• If you are importing exceptions for the first time, click **Download sample CSV**, save and populate the CSV file with objects (see the instructions in the CSV file), browse and then select the CSV file.<br>• If you have imported exceptions previously, save another copy of the CSV file, populate it with new objects, browse and then select the CSV file. |
| Delete/Delete All | Select one or several objects to remove and then click **Delete**.<br>Click **Delete All** to delete all the objects. |
| Export/Export All | Select one or several objects and then click **Export** to save the objects to a CSV file.<br>Click **Export All** to save all the objects to a CSV file. |
| Data Filters | If there are too many entries in the table, limit the entries by performing these tasks:<br>• Select an object type in the **Show** drop-down box.<br>• Select a column name in the **Search column** drop-down box and then type some characters in the **Search keyword** text box next to it. As you type, the entries that match the characters you typed are displayed. TippingPoint Advanced Threat Protection Analyzer searches only the selected column in the table for matches. |
| Records and Pagination Controls | The panel at the bottom of the screen shows the total number of objects. If all the objects cannot be displayed at the same time, use the pagination controls to view the objects that are hidden from view. |

# Sandbox Management

The **Sandbox Management** screen includes the following:

- *Status Tab on page 4-26*

- *Images Tab on page 4-28*
- *YARA Tab on page 4-31*
- *Archive Passwords Tab on page 4-35*
- *Submission Settings Tab on page 4-36*
- *Network Connection Tab on page 4-40*
- *Smart Feedback Tab on page 4-42*
- *Cloud Sandbox Tab on page 4-43*


**Note**

If Virtual Analyzer does not contain images, clicking **Sandbox Management** displays the **Images** tab.

## Status Tab

The **Status** tab displays the following information:

- Overall status of Virtual Analyzer, including the number of samples queued and currently processing

  Virtual Analyzer displays the following:

**TABLE 4-9. Virtual Analyzer Statuses**

| STATUS | DESCRIPTION |
|---|---|
| Initializing... | Virtual Analyzer is preparing the analysis environment. |
| Starting... | Virtual Analyzer is starting all sandbox instances. |
| Stopping... | Virtual Analyzer is stopping all sandbox instances. |
| Running | Virtual Analyzer is analyzing or ready to analyze samples. |
| No images | No images have been imported into Virtual Analyzer. |
| No active images | None of the imported images are currently active. Virtual Analyzer is not analyzing samples. |
| Disabled | Virtual Analyzer is temporarily unavailable. |
| Modifying instances… | Virtual Analyzer is increasing or decreasing the number of instances for one or more images. |
| Importing images… | Virtual Analyzer is importing one or more images. |
| Removing images… | Virtual Analyzer is removing one or more images. |
| Unrecoverable error | Virtual Analyzer is unable to recover from an error. Contact your support provider for troubleshooting assistance. |

- Status of imported images

**Image Status** Idle Busy

| Image | Instances | Current status | | Utilization |
|---|---|---|---|---|
| | | Idle | Busy | |
| winxp | 10 | 5 | 5 | 50% |
| win2k8 | 13 | 7 | 6 | 46% |
| win7 | 10 | 5 | 5 | 50% |
| **All Images** | **33** | **17** | **16** | **48%** |

**TABLE 4-10. Image Information**

| STATUS | DESCRIPTION |
|---|---|
| Image | Permanent image name |
| Instances | Number of deployed sandbox instances |
| Current Status | Distribution of idle and busy sandbox instances |
| Utilization | Overall utilization (expressed as a percentage) based on the number of sandbox instances currently processing samples |

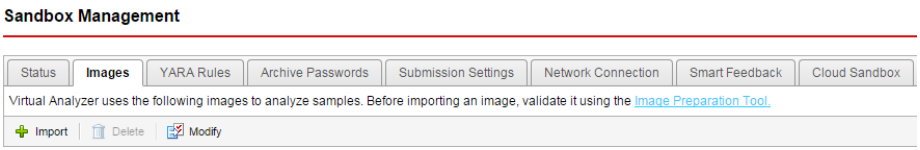
## Images Tab

Virtual Analyzer does not contain any images by default. To analyze samples, you must prepare and import at least one image in the Open Virtual Appliance (OVA) format.

You can use existing VirtualBox or VMware images, or create new images using VirtualBox. For details, see Chapters 2 and 3 of the *Virtual Analyzer Image Preparation User's Guide* at http://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx.

Before importing, validate and configure images using the Virtual Analyzer Image Preparation Tool. For details, see Chapter 4 of the *Virtual Analyzer Image Preparation User's Guide*.

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.



## Importing an Image

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

Virtual Analyzer supports OVA files up to 20GB in size.

**Important**

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

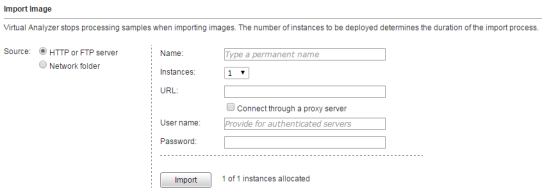
### Procedure

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

   The **Images** screen appears.

2. Click **Import**.

   The **Import Image** screen appears.




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

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

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

   **Note**

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

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

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

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

4. Click **Import**.

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

> **Note**
>
> If you selected **HTTP or FTP server**, TippingPoint Advanced Threat Protection Analyzer downloads the images first before importing into Virtual Analyzer. The process can only be canceled before the download completes.

## Modifying Sandbox Instances

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.

> **Important**
>
> Virtual Analyzer stops all analysis and keeps all samples in the queue whenever an image is added or deleted, or when instances are modified. All instances are also automatically redistributed whenever you add images.

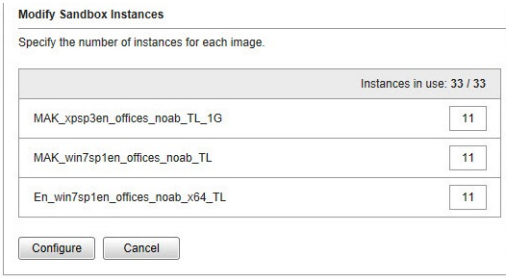
### Procedure

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

   The **Images** screen appears.

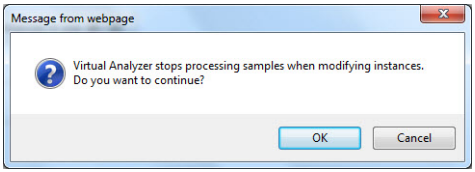
2. Click **Modify**.

The **Modify Sandbox Instances** screen appears.




3. Modify the instances allocated to any image.
4. Click **Configure**.

   Virtual Analyzer displays a confirmation message.




5. Click **OK**.

   Virtual Analyzer configures the sandbox instances. Please wait for the process to finish before navigating away from the screen.

**Note**

If configuration is unsuccessful, Virtual Analyzer reverts to the previous settings and displays an error message.

## YARA Rules tab

Virtual 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. TippingPoint Advanced Threat Protection Analyzer supports a maximum of 5,000 YARA rules regardless of the number of YARA rule files.

The following columns show information about YARA rule files.

**TABLE 4-11. YARA columns**

| COLUMN NAME | INFORMATION |
|---|---|
| File name | Name of the YARA rule file |
| Rules contained | Number of YARA rules contained in the YARA rule file |
| Files to analyze | File types to analyze using the YARA rules in the YARA rule file |
| Added | Date and time the YARA rule file was added |

The following table lists all the YARA Rules tab tasks:

**TABLE 4-12. YARA Rules Tasks**

| TASK | STEPS |
|---|---|
| Add | Browse and select a YARA rule file and the file types to analyze. For details, see *Adding a YARA Rule File on page 4-34*. |
| Delete | Select one or several YARA rule files to remove and then click **Delete**. |
| Records and Pagination Controls | The panel at the bottom of the screen shows the total number of YARA rule files. If all samples cannot display at the same time, use the pagination controls to view the samples that are hidden from view. |

## Creating a YARA Rule File

TippingPoint Advanced Threat Protection Analyzer supports YARA rules that follow version 3.3.0 of the official specifications. YARA rules are stored in plain text files that can be created using any text editor.

For more information about writing YARA rules, visit http://yara.readthedocs.org/en/v3.3.0/writingrules.html.

A YARA rule file must fulfill certain requirements before it can be added to Virtual Analyzer for malware detection:

- File name must be unique
- File content cannot be empty
- Rule names must be unique between all uploaded YARA rule files

The following example shows a simple YARA rule:

```
rule NumberOne
{
meta:
desc = "Sonala"
weight = 10
strings:
$a = {6A 40 68 00 30 00 00 6A 14 8D 91}
$b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
$c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
condition:
$a or $b or $c
}
```

The following table lists the different parts of the YARA rule and how they are used:

**TABLE 4-13. YARA Rule Parts and Usage**

| PART | USAGE |
|---|---|
| rule | The YARA rule name. Must be unique and cannot contain spaces. |
| meta: | Indicates that the "meta" section begins. Parts in the meta section do not affect detection. |
| desc | Optional part that can be used to describe the rule. |

| PART | USAGE |
|---|---|
| weight | Optional part that must be between 1 and 10 that determines the risk level if rule conditions are met:<br>• 1 to 9 = Low risk<br>• 10 = High risk<br>**Note**<br>Virtual Analyzer automatically assigns a value of 10 if no weight is specified. |
| strings: | Indicates that the "strings" section begins. Strings are the main means of detecting malware. |
| $a / $b / $c | Strings used to detect malware. Must begin with a $ character followed by one of more alphanumeric characters and underscores. |
| condition: | Indicates that the "condition" section begins. Conditions determine how your strings are used to detect malware. |
| $a or $b or $c | Conditions are Boolean expressions that define the logic of the rule. They tell the condition under which a submitted object satisfies the rule or not. Conditions can range from the typical Boolean operators `and`, `or` and `not`, to relational operators `>=`, `<=`, `<`, `>`, `==` and `!=`. Arithmetic operators (`+`, `-`, `*`, `\`, `%`) and bitwise operators (`&`, `\|`, `<<`, `>>`, `~`, `^`) can be used on numerical expressions. |

## Adding a YARA Rule File

### Procedure

1. Click **Add** to add a YARA rule file.

   The **Add YARA Rule File** window appears.

2. In the new window that opens, configure the following:

   a. **Rule file**: Browse and select a YARA rule file to add.

b. **Files to analyze**: Specify the file types that Virtual Analyzer processes specific to this YARA rule file.

3. Click **Add** when you have selected the YARA rule file to add and the file types to analyze.

   Virtual Analyzer validates the YARA rule file before adding it. For details about creating valid YARA rule files, see *Creating a YARA Rule File on page 4-32*.

## Archive Passwords Tab

Always handle potentially malicious files with caution. Trend Micro recommends adding such files to a password-protected archive file before transporting the files across the network. TippingPoint Advanced Threat Protection Analyzer can also heuristically discover passwords in email messages to extract files.

Virtual Analyzer uses user-specified passwords to extract files. For better performance, list commonly used passwords first.

Virtual Analyzer supports the following archive file types:

- `bzip`
- `rar`
- `tar`
- `zip`

If Virtual Analyzer is unable to extract files using any of the listed passwords, TippingPoint Advanced Threat Protection Analyzer displays the error Unsupported file type and removes the archive file from the queue.

**Note**

Archive file passwords are stored as unencrypted text.

## Adding Archive Passwords

TippingPoint Advanced Threat Protection Analyzer supports a maximum of 10 passwords.

---

**Procedure**

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

   The **Archive Passwords** screen appears.

2. Type a password with only ASCII characters.

   **Note**

   Passwords are case-sensitive and must not contain spaces.

3. Optional: Click **Add password** and type another password.
4. Optional: Drag and drop the password to move it up or down the list.
5. Optional: Delete a password by clicking the x icon beside the corresponding text box.
6. Click **Save**.

---

# Submission Settings Tab

Use the **Submission Settings** tab, in **Virtual Analyzer** > **Sandbox Management**, to view or specify the file types that Virtual Analyzer processes.

Trend Micro identifies files by true file type and not by extension. Sample file extensions are provided for reference.

**TABLE 4-14. Virtual Analyzer File Types**

| DISPLAYED FILE EXTENSION | FULL FILE TYPE |
|---|---|
| cell | Hancom™ Hancell spreadsheet |
| chm | Compiled HTML (CHM) help file |
| class | Java™ Class file |
| dll | AMD™ 64-bit DLL file<br>Microsoft™ Windows™ 16-bit DLL file<br>Microsoft™ Windows™ 32-bit DLL file |
| doc | Microsoft™ Word™ document |
| docx | Microsoft™ Office Word™ 2007 Document |

| Displayed File Extension | Full File Type |
|---|---|
| exe | Executable file (EXE)<br>AMD™ 64-bit EXE file<br>DIET DOS EXE file<br>Microsoft™ DOS EXE file<br>IBM™ OS/2 EXE file<br>LZEXE DOS EXE file<br>MIPS EXE file<br>MSIL Portable executable file<br>Microsoft™ Windows™ 16-bit EXE file<br>Microsoft™ Windows™ 32-bit EXE file<br>ARJ compressed EXE file<br>ASPACK 1.x compressed 32-bit EXE file<br>ASPACK 2.x compressed 32-bit EXE file<br>GNU UPX compressed EXE file<br>LZH compressed EXE file<br>LZH compressed EXE file for ZipMail<br>MEW 0.5 compressed 32-bit EXE file<br>MEW 1.0 compressed 32-bit EXE file<br>MEW 1.1 compressed 32-bit EXE file<br>PEPACK compressed executable<br>PKWARE™ PKLITE™ compressed DOS EXE file<br>PETITE compressed 32-bit executable file<br>PKZIP compressed EXE file<br>WWPACK compressed executable file |
| gul | JungUm™ Global document |

| Displayed File Extension | Full File Type |
|---|---|
| hwp | Hancom™ Hangul Word Processor (HWP) document |
| hwpx | Hancom™ Hangul Word Processor 2014 (HWPX) document |
| jar | Java™ Applet<br>Java™ Application |
| js | JavaScript™ file |
| jse | JavaScript™ encoded script file |
| jtd | JustSystems™ Ichitaro™ document |
| lnk | Microsoft™ Windows™ Shell Binary Link shortcut |
| mov | Apple™ QuickTime™ media |
| pdf | Adobe™ Portable Document Format (PDF) |
| ppt | Microsoft™ Powerpoint™ presentation |
| pptx | Microsoft™ Office PowerPoint™ 2007 Presentation |
| ps1 | Microsoft™ Windows™ PowerShell script file |
| rtf | Microsoft™ Rich Text Format (RTF) document |
| swf | Adobe™ Shockwave™ Flash file |
| vbe | Visual Basic™ encoded script file |
| vbs | Visual Basic™ script file |
| xls | Microsoft™ Excel™ spreadsheet |
| xlsx | Microsoft™ Office Excel™ 2007 Spreadsheet |
| xml | Microsoft™ Office 2003 XML file |

**TABLE 4-15. Submission Settings Tab Tasks**

| TASK | STEPS |
|---|---|
| Move to the **Analyzed** list | 1. Select one or more file types in the **Not analyzed** list.<br>2. Click **>>**.<br>3. Click **Save**. |
| Move to the **Not analyzed** list | 1. Select one or more file types in the **Analyzed** list.<br>2. Click **<<**.<br>3. Click **Save**. |
| Restore the default settings | Click **Restore Default**. |

## Network Connection Tab

Use the **Network Connection** tab to specify how sandbox instances connect to external destinations.

External connections are disabled by default. Trend Micro recommends enabling external connections using an environment isolated from the management network. The environment can be a test network with Internet connection but without proxy settings, proxy authentication, and connection restrictions.

When external connections are enabled, any malicious activity involving the Internet and remote hosts actually occurs during sample processing.

### Enabling External Connections

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

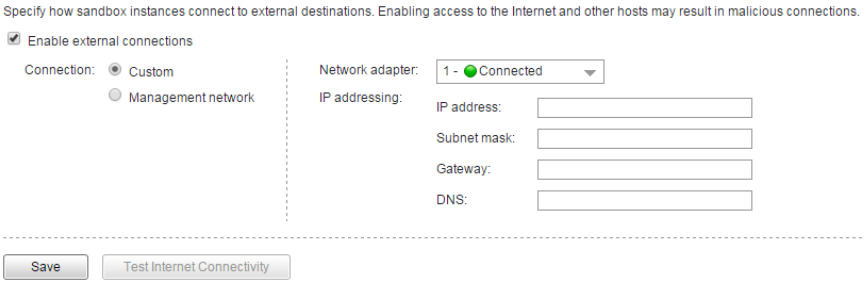
**Procedure**

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.




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**.

## Testing Internet Connectivity

Verify Internet connectivity after enabling the external connection and configuring the settings.

**Procedure**

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Network Connection** tab.
2. Click **Test Internet Connectivity**.

Note

**Test Internet Connectivity** will be disabled if external connections are not enabled or the settings are not saved.

# Smart Feedback Tab

TippingPoint Advanced Threat Protection Analyzer integrates the Trend Micro Feedback Engine. This engine sends anonymous threat information to the Trend Micro Smart Protection Network, which allows Trend Micro to identify and protect against new threats. Enabling Smart Feedback authorizes Trend Micro to collect the following information from your network, which is kept in strict confidence.

- Product ID and version
- URLs suspected to be fraudulent or possible sources of threats
- File type and SHA-1 hash value of detected files

### Enabling Smart Feedback

**Procedure**

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Smart Feedback** tab.
2. Configure Smart Feedback settings.
   a. Select **Enable Smart Feedback (recommended)** to send anonymous threat information to Trend Micro from your network.
   b. Select **Submit suspicious executable files to Trend Micro** to send high-risk files to Trend Micro for further investigation.

## Cloud Sandbox Tab

When the cloud sandbox setting is enabled, TippingPoint Advanced Threat Protection Analyzer sends possible Mac OS threats to Trend Micro cloud sandboxes for analysis.

### Enabling Cloud Sandbox

Before enabling the could sandbox, verify that TippingPoint Advanced Threat Protection Analyzer has an Internet connection.

**Note**

In a cluster environment, the cloud sandbox setting does not propagate from the primary appliance. Enable the cloud sandbox setting on the management console of each secondary appliance.

**Important**

The cloud sandbox setting is automatically disabled if the TippingPoint Advanced Threat Protection Analyzer license expires.

**Procedure**

1. Go to **Virtual Analyzer** > **Sandbox Management** and click the **Cloud Sandbox** tab.
2. Select **Send possible Mac OS threats to the Trend Micro cloud sandboxes for analysis**.
3. Click **Save**.

# Submitters

Use the **Submitters** screen, in **Virtual Analyzer** > **Submitters**, to adjust Virtual Analyzer resource allocation between all sources that submit objects to TippingPoint Advanced Threat Protection Analyzer for analysis. Virtual Analyzer utilizes more resources to process submissions by submitters with higher weight settings.

The following columns show information about submitters, average processing time, total submissions, and total resources allocated to submitters. Columns for the adjustment of weight and removal of submitters are provided as well.

**TABLE 4-16. Submitters Columns**

| COLUMN NAME | INFORMATION / ACTION |
|---|---|
| Submitter | Name of the Trend Micro product that submits the objects |
| Host Name | Host name of the Trend Micro product that submits the objects |
| Last Submission | Date and time Virtual Analyzer last received a submission |
| Average Processing Time | Average time it takes Virtual Analyzer to process a submitted object |
| Submissions (% of Total) | Number of objects submitted by the Trend Micro product |
| Weight | Weight setting of the Trend Micro product. Specify a value between 1 and 100 to recalculate resource allocation. |

| Column Name | Information / Action |
|---|---|
| % of Total Resources | Percentage of total Virtual Analyzer resources allocated to the Trend Micro product. |
| Action | Deletes the Trend Micro product from TippingPoint Advanced Threat Protection Analyzer. Deleted products cannot submit new objects for scanning and analysis or query analysis results, but queued objects will be processed and analysis results will be stored.<br><br>**Note**<br>To reintegrate the product, see *Integration with Trend Micro Products and Services on page 2-6*. |

# Chapter 5

# Alerts and Reports

This chapter describes the features of **Alerts** and **Reports**.

# Alerts

The **Alerts** screen includes the following:

- Triggered Alerts Tab
- Rules Tab

## Triggered Alerts Tab

The **Triggered Alerts** tab, in **Alerts / Reports** > **Alerts**, shows all alert notifications generated by TippingPoint Advanced Threat Protection Analyzer. Alert notifications provide immediate intelligence about the state of TippingPoint Advanced Threat Protection Analyzer.

The following columns show information about alert notifications created by TippingPoint Advanced Threat Protection Analyzer:

**TABLE 5-1. Triggered Alerts Columns**

| COLUMN NAME | INFORMATION |
|---|---|
| Triggered | Date and Time TippingPoint Advanced Threat Protection Analyzer triggered the alert notification. |
| Level | Level of the triggered alert notification.<br>• **Critical**: The event requires immediate attention<br>• **Important**: The event requires observation<br>• **Informational**: The event requires limited observation |
| Rule | Rule that triggered the alert notification. |
| Affected Appliance | Host name, IPv4 and IPv6 addresses of the appliance affected by the alert notification content, if applicable. |
| Details | Click the icon to view the full alert notification details, including the list of notification recipients, subject, and message of the alert notification. |

## Rules Tab

The **Rules** tab, in **Alerts / Reports** > **Alerts**, shows all alert notification rules used by TippingPoint Advanced Threat Protection Analyzer.

The following columns show information about the alert notification rules used by TippingPoint Advanced Threat Protection Analyzer:

**TABLE 5-2. Rules Columns**

| COLUMN NAME | INFORMATION |
|---|---|
| Alert Level | Level of the alert notification rule.<br>• **Critical**: The event requires immediate attention<br>• **Important**: The event requires observation<br>• **Informational**: The event requires limited observation |
| Rule | Rule that triggers the alert notification. |
| Criteria | Description of the alert rule. |
| Alert Frequency | Frequency at which the alert notification is sent if threshold is reached or exceeded. |
| Status | Click the toggle to enable or disable the rule. |

The threshold to trigger each alert is configurable. For details, see *Modifying Rules on page 5-6*

### Critical Alerts

The following table explains the critical alerts triggered by events requiring immediate attention. TippingPoint Advanced Threat Protection Analyzer considers malfunctioning sandboxes and appliances as critical problems.

**TABLE 5-3. Critical Alerts**

| NAME | CRITERIA (DEFAULT) | ALERT FREQUENCY (DEFAULT) |
|---|---|---|
| Virtual Analyzer Stopped | Virtual Analyzer encountered an error and was unable to recover. Analysis has stopped. | Immediate |
| Passive Primary Appliance Activated | The active primary appliance encountered an error and was unable to recover. The passive primary appliance took over the active role. | Immediate |

## Important Alerts

The following table explains the important alerts triggered by events that require observation. TippingPoint Advanced Threat Protection Analyzer considers suspicious object detections, hardware capacity changes, certain sandbox queue activity, component update, account and clustering issues as important problems.

**TABLE 5-4. Important Alerts**

| NAME | CRITERIA (DEFAULT) | ALERT FREQUENCY (DEFAULT) |
|---|---|---|
| Account Locked | An account was locked because of multiple unsuccessful logon attempts. | Immediate |
| Long Virtual Analyzer Queue | The Virtual Analyzer queue has exceeded the specified threshold. | Once every 30 minutes |
| Component Update Unsuccessful | A component update was unsuccessful. | Once every 30 minutes |
| High CPU Usage | The average CPU usage in the last 5 minutes has exceeded the specified threshold. | Once every 30 minutes |

| Name | Criteria (Default) | Alert Frequency (Default) |
|---|---|---|
| High Memory Usage | The average memory usage in the last 5 minutes has exceeded the specified threshold. | Once every 30 minutes |
| High Disk Usage | The disk usage has exceeded the specified threshold. | Once every 30 minutes |
| Secondary Appliance Unresponsive | A secondary appliance in the cluster encountered an error and was unable to recover. | Immediate |
| High Availability Suspended | The passive primary appliance encountered an error and was unable to recover. High availability was suspended. | Once every 30 minutes |
| New High-Risk Objects Identified | The number of new high-risk objects identified over the specified time period has reached the specified threshold. | Immediate |

## Informational Alerts

The following table explains the alerts triggered by events that require limited observation. TippingPoint Advanced Threat Protection Analyzer considers restoration of high availability, and inaccessibility of syslog and backup servers as informational events.

**Table 5-5. Informational Alerts**

| Name | Criteria (Default) | Alert Frequency (Default) |
|---|---|---|
| Syslog Server Inaccessible | The syslog server was inaccessible. Logs were not sent to the server. | Once every 30 minutes |
| Backup Server Inaccessible | The backup server was inaccessible. Logs and objects were not backed up. | Once every 30 minutes |

| Name | Criteria (Default) | Alert Frequency (Default) |
|---|---|---|
| High Availability Restored | The passive primary appliance recovered from an error and high availability was restored. | Immediate |

## Modifying Rules

### Before you begin

Configure the SMTP server to send notifications. For details, see *SMTP Tab on page 6-17*.

All triggered alert rules can notify recipients with a custom email message. Some rules have additional parameters, including object count, submission count, or time period. Trend Micro recommends adding at least one notification recipient for all critical and important alerts.

---

**Procedure**

1. Go to **Alerts / Reports** > **Alerts** > **Rules**

   The **Rules** screen appears.

2. Click the name of an alert rule under the **Rule** column.

   The alert rule configuration screen appears.

3. Modify the rule settings.

   **Note**

   For details, see *Alert Notification Parameters on page 5-7*.

4. Click **Save**.

---

## Alert Notification Parameters

All triggered alert rules can notify recipients with a custom email message. Some rules have additional parameters, including object count, submission count, or time period.

### Critical Alert Parameters

**Note**

For explanations about available message tokens in each alert, see *Alert Notification Message Tokens on page 5-19*.

**TABLE 5-6. Virtual Analyzer Stopped**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Alert frequency | Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified. |
| Subject | Specify the subject of the triggered alert notification. |
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%ApplianceName%`<br>• `%ApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

**TABLE 5-7. Passive Primary Appliance Activated**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Alert frequency | Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified. |
| Subject | Specify the subject of the triggered alert notification. |
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%ActiveApplianceName%`<br>• `%ActiveApplianceIP%`<br>• `%PassiveApplianceName%`<br>• `%PasssiveApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

## Important Alert Parameters

**Note**

For explanations about available message tokens in each alert, see *Alert Notification Message Tokens on page 5-19*.

**TABLE 5-8. Account Locked**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select to enable or disable this alert. |

| Parameter | Description |
|---|---|
| Alert level | Shows the level of this alert. Cannot be modified. |
| Alert frequency | Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified. |
| Subject | Specify the subject of the triggered alert notification. |
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%LockedAccount%`<br>• `%ApplianceName%`<br>• `%ApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

**Table 5-9. Long Virtual Analyzer Queue**

| Parameter | Description |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Submissions | Specify the submissions threshold that will trigger the alert.<br>**Tip**<br>Refer to the red line of the **Queued Samples** widget to see the estimated number of samples Virtual Analyzer can analyze within 5 minutes. For details, see *Queued Samples on page 3-13*. |
| Alert frequency | Select the frequency at which this alert is sent when rule criteria are met. |

| Parameter | Description |
|---|---|
| Subject | Specify the subject of the triggered alert notification. |
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%SandboxQueueThreshold%`<br>• `%SandboxQueue%`<br>• `%ApplianceName%`<br>• `%ApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

**Table 5-10. Component Update Unsuccessful**

| Parameter | Description |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Alert frequency | Select the frequency at which this alert is sent when rule criteria are met. |
| Subject | Specify the subject of the triggered alert notification. |

| Parameter | Description |
|---|---|
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%ComponentList%`<br>• `%UpdateError%`<br>• `%ApplianceName%`<br>• `%ApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

**Table 5-11. High CPU Usage**

| Parameter | Description |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Average CPU usage | Specify the average CPU usage threshold that will trigger the alert. |
| Alert frequency | Select the frequency at which this alert is sent when rule criteria are met. |
| Subject | Specify the subject of the triggered alert notification. |

| Parameter | Description |
|---|---|
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%CPUThreshold%`<br>• `%CPUUsage%`<br>• `%ApplianceName%`<br>• `%ApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

**Table 5-12. High Memory Usage**

| Parameter | Description |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Average memory usage | Specify the average memory usage threshold that will trigger the alert. |
| Alert frequency | Select the frequency at which this alert is sent when rule criteria are met. |
| Subject | Specify the subject of the triggered alert notification. |

| Parameter | Description |
|---|---|
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%MemThreshold%`<br>• `%MemUsage%`<br>• `%ApplianceName%`<br>• `%ApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

**Table 5-13. High Disk Usage**

| Parameter | Description |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Disk usage | Specify the disk usage threshold that will trigger the alert. |
| Alert frequency | Select the frequency at which this alert is sent when rule criteria are met. |
| Subject | Specify the subject of the triggered alert notification. |

| Parameter | Description |
|---|---|
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%ApplianceName%`<br>• `%ApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

**Table 5-14. Secondary Appliance Unresponsive**

| Parameter | Description |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Alert frequency | Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified. |
| Subject | Specify the subject of the triggered alert notification. |
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%ApplianceError%`<br>• `%ApplianceName%`<br>• `%ApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

**TABLE 5-15. High Availability Suspended**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Alert frequency | Select the frequency at which this alert is sent when rule criteria are met. |
| Subject | Specify the subject of the triggered alert notification. |
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%ActiveApplianceName%`<br>• `%ActiveApplianceIP%`<br>• `%PassiveApplianceName%`<br>• `%PasssiveApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

**TABLE 5-16. New High-Risk Objects Identified**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Objects | Specify the objects threshold that will trigger the alert.<br>**Note**<br>Specifying a low threshold may result in frequent generation of alerts, but each alert covers a unique set of detections. |

| Parameter | Description |
|---|---|
| Alert frequency | Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified. |
| Time period | Specify the time period threshold that will trigger the alert.<br><br>**Note**<br>Specifying a low threshold may result in frequent generation of alerts, but each alert covers a unique set of detections. |
| Subject | Specify the subject of the triggered alert notification. |
| Message | Specify the body of the triggered alert notification.<br><br>Use the following tokens to customize your message:<br><br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%HighRiskThreshold%`<br>• `%TimeRange%`<br>• `%ApplianceName%`<br>• `%ApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

## Informational Alert Parameters

**Note**

For explanations about available message tokens in each alert, see *Alert Notification Message Tokens on page 5-19*.

**TABLE 5-17. Syslog Server Inaccessible**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Alert frequency | Select the frequency at which this alert is sent when rule criteria are met. |
| Subject | Specify the subject of the triggered alert notification. |
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%SyslogServer%`<br>• `%ApplianceName%`<br>• `%ApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

**TABLE 5-18. Backup Server Inaccessible**

| PARAMETER | DESCRIPTION |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Alert frequency | Select the frequency at which this alert is sent when rule criteria are met. |
| Subject | Specify the subject of the triggered alert notification. |

| Parameter | Description |
|---|---|
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%BackupServer%`<br>• `%ApplianceName%`<br>• `%ApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

**Table 5-19. High Availability Restored**

| Parameter | Description |
|---|---|
| Status | Select to enable or disable this alert. |
| Alert level | Shows the level of this alert. Cannot be modified. |
| Alert frequency | Shows the frequency at which this alert is sent when rule criteria are met. Cannot be modified. |
| Subject | Specify the subject of the triggered alert notification. |

| Parameter | Description |
|---|---|
| Message | Specify the body of the triggered alert notification.<br>Use the following tokens to customize your message:<br>• `%ProductName%`<br>• `%ProductShortName%`<br>• `%ActiveApplianceName%`<br>• `%ActiveApplianceIP%`<br>• `%PassiveApplianceName%`<br>• `%PasssiveApplianceIP%`<br>• `%DateTime%`<br>• `%ConsoleURL%` |

## Alert Notification Message Tokens

The following table explains the tokens available for alert notifications. Use the table to understand which alert rules accept the message token and the information that the token provides in an alert notification.

**Note**

Not every alert notification can accept every message token. Review the alert's parameter specifications before using a message token. For details, see *Alert Notification Parameters on page 5-7*.

**TABLE 5-20. Message Tokens**

| TOKEN | DESCRIPTION | EXAMPLE | WHERE ALLOWED |
|---|---|---|---|
| `%ActiveApplianceIP%` | The IP address of the TippingPoint Advanced Threat Protection Analyzer active primary appliance | 123.123.123.123 \| 2001:0:3238:DFE1:63::FEFB | High Availability Restored<br>High Availability Suspended<br>Passive Primary Appliance Activated |
| `%ActiveApplianceName%` | The host name of the TippingPoint Advanced Threat Protection Analyzer active primary appliance | • ATP_Analyzer<br>• ATP_Analyzer-ABC123 | High Availability Restored<br>High Availability Suspended<br>Passive Primary Appliance Activated |
| `%ApplianceError%` | The error encountered by the appliance | • Inconsistent component version<br>• Not connected<br>• Invalid API key<br>• Incompatible software version | Secondary Appliance Unresponsive |
| `%ApplianceIP%` | The IP address of the TippingPoint Advanced Threat Protection Analyzer appliance | 123.123.123.123 \| 2001:0:3238:DFE1:63::FEFB | All<br>• High Availability Restored<br>• High Availability Suspended<br>• Passive Primary Appliance Activated |

| Token | Description | Example | Where Allowed |
|---|---|---|---|
| `%ApplianceName%` | The host name of the TippingPoint Advanced Threat Protection Analyzer appliance | • ATP_Analyzer<br>• ATP_Analyzer-ABC123 | All<br>• High Availability Restored<br>• High Availability Suspended<br>• Passive Primary Appliance Activated |
| `%BackupServer%` | The host name or IP address of the backup server | • my.example.com<br>• 123.123.123.123<br>• 2001:0:3238:DFE1:63::FEFB | Backup Server Inaccessible |
| `%ComponentList%` | The list of components | • Advanced Threat Scan Engine<br>• Deep Discovery Malware Pattern<br>• IntelliTrap Exception Pattern<br>• IntelliTrap Pattern | Component Update Unsuccessful |
| `%ConsoleURL%` | The TippingPoint Advanced Threat Protection Analyzer management console URL | https://192.168.85.69/ \| https://[2001:0:3238:DFE1:63::FEFB]/ | All |

| Token | Description | Example | Where Allowed |
|---|---|---|---|
| `%CPUThreshold%` | The average CPU usage as a percentage allowed in the last 5 minutes before TippingPoint Advanced Threat Protection Analyzer sends an alert notification | 80% | High CPU Usage |
| `%CPUUsage%` | The total CPU usage as a percentage in the last 5 minutes | 80% | High CPU Usage |
| `%DateTime%` | The date and time the alert was initiated | 2014-03-21 03:34:09 | All |
| `%DiskThreshold%` | The disk usage as a percentage allowed before TippingPoint Advanced Threat Protection Analyzer sends an alert notification | 85% | High Disk Usage |
| `%DiskUsage%` | The total disk usage as a percentage | 85% | High Disk Usage |
| `%FreeDiskSpace%` | The amount of free disk space in GB | 50GB | High Disk Usage |
| `%HighRiskThreshold%` | The maximum number of new high-risk objects identified during the specified time period before TippingPoint Advanced Threat Protection Analyzer sends an alert notification | 10 | New High-Risk Objects Identified |
| `%LockedAccount%` | The account that was locked | guest | Account Locked |

| Token | Description | Example | Where Allowed |
|---|---|---|---|
| `%MemThreshold%` | The average memory usage as a percentage allowed in the last 5 minutes before TippingPoint Advanced Threat Protection Analyzer sends an alert notification | 90% | High Memory Usage |
| `%MemUsage%` | The total memory usage as a percentage in the last 5 minutes | 90% | High Memory Usage |
| `%PasssiveAppliance IP%` | The IPv4 address of the TippingPoint Advanced Threat Protection Analyzer passive primary appliance | 123.123.123.123 | High Availability Restored<br>High Availability Suspended<br>Passive Primary Appliance Activated |
| `%PassiveAppliance Name%` | The host name of the TippingPoint Advanced Threat Protection Analyzer passive primary appliance | • ATP_Analyzer<br>• ATP_Analyzer-ABC123 | High Availability Restored<br>High Availability Suspended<br>Passive Primary Appliance Activated |
| `%ProductName%` | The product name | TippingPoint Advanced Threat Protection Analyzer | All |
| `%ProductShortName%` | The abbreviated product name | ATP Analyzer | All |
| `%SandboxQueue%` | The submission count in the sandbox queue waiting to be analyzed by Virtual Analyzer | 100 | Long Virtual Analyzer Queue |

| Token | Description | Example | Where Allowed |
|---|---|---|---|
| `%SandboxQueueThreshold%` | The maximum number of submissions in the sandbox queue before TippingPoint Advanced Threat Protection Analyzer sends an alert notification | 30 | Long Virtual Analyzer Queue |
| `%SyslogServer%` | The host name or IP address of the syslog server | • my.example.com<br>• 123.123.123.123<br>• 2001:0:3238:DFE1:63::FEFB | Syslog Server Inaccessible |
| `%TimeRange%` | The time period observed for new high-risk objects before TippingPoint Advanced Threat Protection Analyzer sends an alert notification | • 5 minutes<br>• 30 minutes<br>• 1 hour<br>• 12 hours<br>• 24 hours | New High-Risk Objects Identified |

| Token | Description | Example | Where Allowed |
|---|---|---|---|
| `%UpdateError%` | The list of update errors | • Unable to download: Advanced Threat Scan Engine<br>• Unable to update: Deep Discovery Malware Pattern<br>• Unable to update: IntelliTrap Exception Pattern. The appliance is configuring Virtual Analyzer instances or shutting down. | Component Update Unsuccessful |

# Reports

All reports generated by TippingPoint Advanced Threat Protection Analyzer are based on an operational report template.

## Generated Reports Tab

The **Generated Reports** tab, in **Alerts / Reports** > **Reports** > **Generated Reports**, shows all reports generated by TippingPoint Advanced Threat Protection Analyzer.

In addition to being displayed as links on the management console, generated reports are also available as attachments to an email. Before generating a report, you are given the option to send it to one or several email recipients.

## Report Tasks

The **Generated Reports** screen includes the following options:

**TABLE 5-21. Generated Reports Tasks**

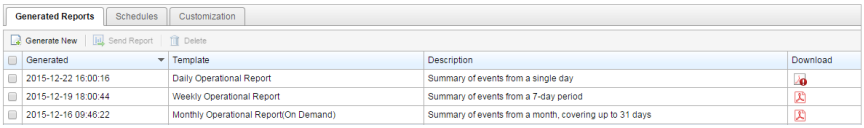
| TASK | STEPS |
|---|---|
| Generate Reports | See *Generating Reports on page 5-26*. |
| Download Report | To download a report, go to the last column in the table and click the icon. Generated reports are available as PDF files. |
| Send Report | Select a report and then click **Send Report**. You can send only one report at a time. |
| Delete | Select one or more reports and then click **Delete**. |
| Sort Column Data | Click a column title to sort the data below it. |
| Records and Pagination Controls | The panel at the bottom of the screen shows the total number of reports. If all reports cannot display at the same time, use the pagination controls to view the reports that are hidden from view. |

## Generating Reports

### Procedure

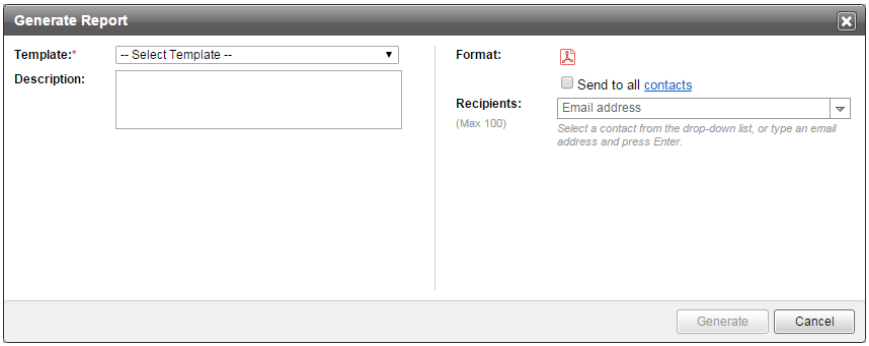
1. Go to **Alerts / Reports** > **Reports** > **Generated Reports**.

   The **Generated Reports** screen appears.



2. Click **Generate New**.

   The **Generate Report** window appears.




3. Configure report settings.

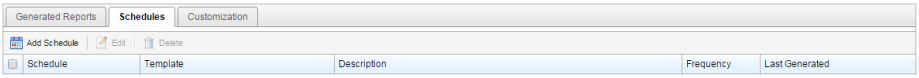
| Option | Description |
|---|---|
| **Template** | Select an operational report template. |
| **Description** | Type a description that does not exceed 500 characters. |
| **Range** | Specify the covered date(s) based on the selected report template.<br>• **Daily operational report**: Select any day prior to the current day. The report coverage is from 00:00:00 to 23:59:59 of each day.<br>• **Weekly operational report**: Select the day of the week on which the report coverage ends. For example, if you choose Wednesday, the report coverage is from Wednesday of a particular week at 23:59:59 until Thursday of the preceding week at 00:00:00.<br>• **Monthly operational report**: Select the day of the month on which the report coverage ends. For example, if you choose the 10th day of a month, the report coverage is from the 10th day of a particular month at 23:59:59 until the 11th day of the preceding month at 00:00:00. |

| Option | Description |
|---|---|
| **Format** | The file format of the report is PDF only. |
| **Send to all contacts** | Select the checkbox to send the generated report to all contacts. |
| **Recipients** | Select a contact from the drop-down list, or type an email address and press ENTER.<br><br>You can type a maximum of 100 email addresses, typing them one at a time.<br><br>**Note**<br>You must press ENTER after each email address. Do not type multiple email addresses separated by commas.<br><br>Before specifying recipients, configure the SMTP settings in **Administration** > **System Settings** > **SMTP** .<br><br>**Note**<br>TippingPoint Advanced Threat Protection Analyzer generates reports approximately five minutes after **Send** is clicked. |

4. Click **Generate**.

## Schedules Tab

The **Schedules** tab, in **Alerts / Reports** > **Reports** > **Schedules**, shows all the report schedules created from report templates. Each schedule contains settings for reports, including the template that will be used and the actual schedule.



**Note**

This screen does not contain any generated reports. To view the reports, navigate to **Alerts / Reports** > **Reports** > **Schedules**.

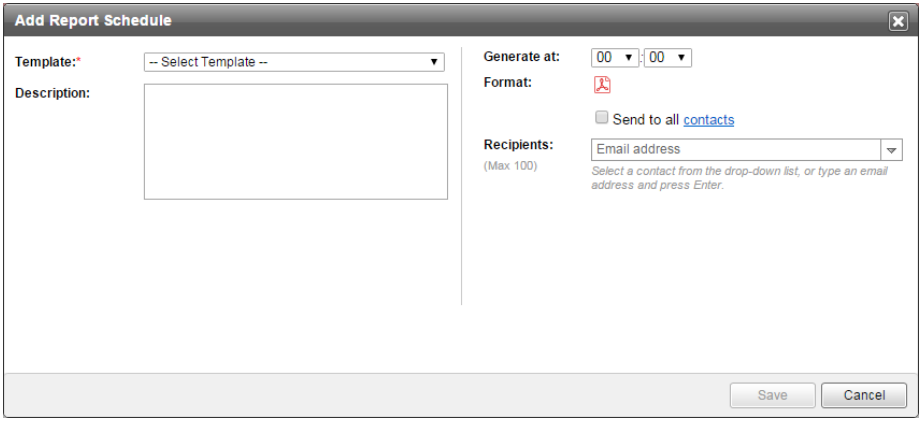
This tab includes the following options:

**TABLE 5-22. Schedules Tasks**

| TASK | STEPS |
|---|---|
| Add Schedule | Click **Add Schedule** to add a new report schedule. This opens the **Add Report Schedule** window, where you specify settings for the report schedule. For details, see *Add Report Schedule Window on page 5-30*. |
| Edit | Select a report schedule and then click **Edit** to edit its settings. This opens the **Edit Report Schedule** window, which contains the same settings in the **Add Report Schedule** window. For details, see *Add Report Schedule Window on page 5-30*.<br><br>Only one report schedule is edited at a time. |
| Delete | Select one or several report schedules to delete and then click **Delete**. |
| Sort Column Data | Click a column title to sort the data below it. |
| Records and Pagination Controls | The panel at the bottom of the screen shows the total number of report schedules. If all report schedules cannot be displayed at the same time, use the pagination controls to view the schedules that are hidden from view. |

## Add Report Schedule Window

The **Add Report Schedule** window appears when you add a report schedule. A report schedule contains settings that TippingPoint Advanced Threat Protection Analyzer will use when generating scheduled reports.




This window includes the following options:

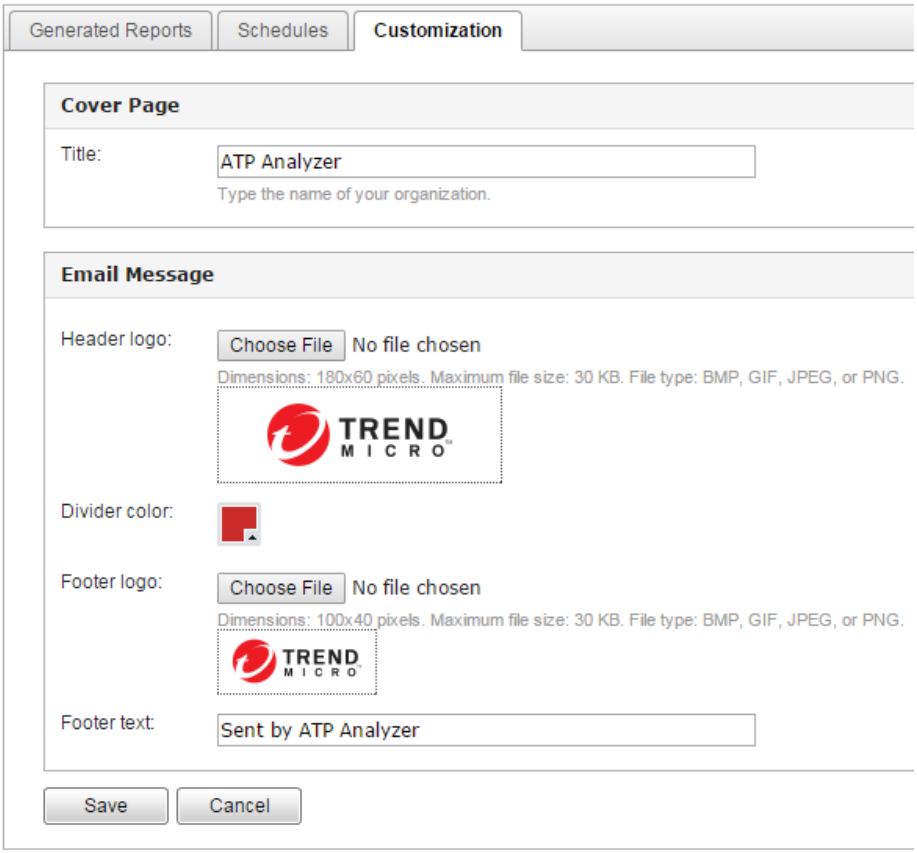
**TABLE 5-23. Add Report Schedule Window Tasks**

| FIELD | STEPS |
|---|---|
| **Template** | Choose a template. |
| **Description** | Type a description. |

| Field | Steps |
|---|---|
| **Generate at** | Configure the schedule according to the template you chose.<br><br>If the template is for a daily report, configure the time the report generates. The report coverage is from 00:00:00 to 23:59:59 of each day and the report starts to generate at the time you specified.<br><br>If the template is for a weekly report, select the start day of the week and configure the time the report generates. For example, if you choose Wednesday, the report coverage is from Wednesday of a particular week at 00:00:00 until Tuesday of the following week at 23:59:59. The report starts to generate on Wednesday of the following week at the time you specified.<br><br>If the template is for a monthly report, select the start day of the month and configure the time the report generates. For example, if you choose the 10th day of a month, the report coverage is from the 10th day of a particular month at 00:00:00 until the 9th day of the following month at 23:59:59. The report starts to generate on the 10th day of the following month at the time you specified.<br><br>**Note**<br>If the report is set to generate on the 29th, 30th, or 31st day of a month and a month does not have this day, TippingPoint Advanced Threat Protection Analyzer starts to generate the report on the first day of the next month at the time you specified. |
| **Format** | The file format of the report is PDF only. |
| **Send to all contacts** | Select the checkbox to send the generated report to all contacts. |
| **Recipients** | Select a contact from the drop-down list, or type a valid email address to which to send reports and then press ENTER. You can type up to 100 email addresses, typing them one at a time. It is not possible to type multiple email addresses separated by commas.<br><br>Before specifying recipients, verify that you have specified SMTP settings in the **SMTP** tab located at **Administration** > **System Settings**. |

## Customization Tab

The **Customization** tab, in **Alerts / Reports** > **Reports** > **Customization**, allows you to customize items in the TippingPoint Advanced Threat Protection Analyzer reports.




This screen includes the following options:

**TABLE 5-24. Cover Page**

| OPTION | TASK | DISPLAY AREA |
|---|---|---|
| Title | Type a title that does not exceed 40 characters. | Report cover |

**TABLE 5-25. Email Message**

| OPTION | TASKS | DISPLAY AREA |
|---|---|---|
| Header logo | Browse to the location of the logo.<br>The following are the image requirements.<br>• Dimensions: 180 x 60 pixels<br>• Maximum file size: 30 KB<br>• File type: `BMP`, `GIF`, `JPG`, or `PNG` | Notification |
| Divider color | To change the default color, click in the box and use the color pick specify a new value.<br> | Notification |
| Footer logo | Browse to the location of the logo.<br>The following are the image requirements.<br>• Dimensions: 100 x 40 pixels<br>• Maximum file size: 30 KB<br>• File type: `BMP`, `GIF`, `JPG`, or `PNG` | Notification |
| Footer text | Type a footer that does not exceed 60 characters. | Notification |

# Chapter 6

# Administration

The features of **Administration** are discussed in this chapter.

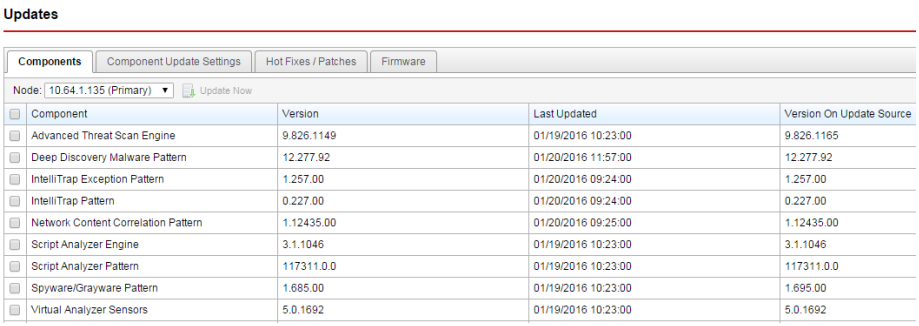
# Updates

Use the **Updates** screen, in **Administration** > **Updates**, to configure component and product update settings.

An Activation Code is required to use and update components. For details, see *License on page 6-51*.

## Components

The **Components** tab shows the security components currently in use.




| Component | Version | Last Updated | Version On Update Source |
|---|---|---|---|
| Advanced Threat Scan Engine | 9.826.1149 | 01/19/2016 10:23:00 | 9.826.1165 |
| Deep Discovery Malware Pattern | 12.277.92 | 01/20/2016 11:57:00 | 12.277.92 |
| IntelliTrap Exception Pattern | 1.257.00 | 01/20/2016 09:24:00 | 1.257.00 |
| IntelliTrap Pattern | 0.227.00 | 01/20/2016 09:24:00 | 0.227.00 |
| Network Content Correlation Pattern | 1.12435.00 | 01/20/2016 09:25:00 | 1.12435.00 |
| Script Analyzer Engine | 3.1.1046 | 01/19/2016 10:23:00 | 3.1.1046 |
| Script Analyzer Pattern | 117311.0.0 | 01/19/2016 10:23:00 | 117311.0.0 |
| Spyware/Grayware Pattern | 1.685.00 | 01/19/2016 10:23:00 | 1.695.00 |
| Virtual Analyzer Sensors | 5.0.1692 | 01/19/2016 10:23:00 | 5.0.1692 |

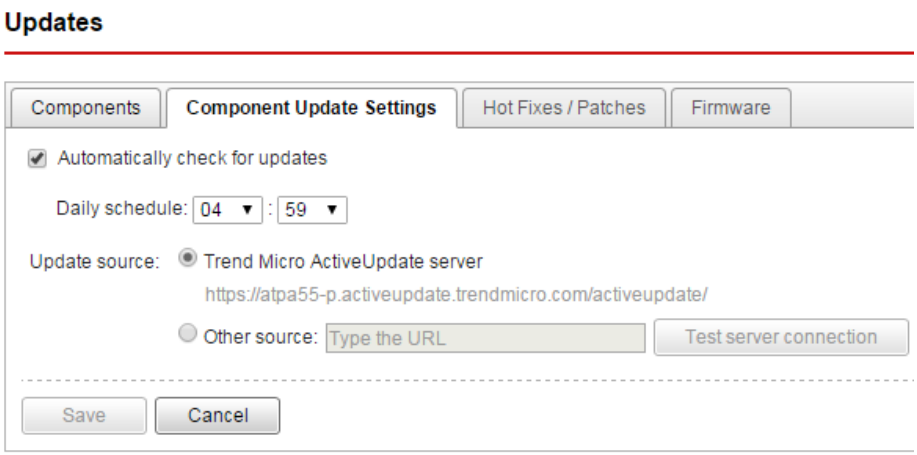
**TABLE 6-1. Components**

| COMPONENT | DESCRIPTION |
|---|---|
| Advanced Threat Scan Engine | The Advanced Threat Scan Engine protects against viruses, malware, and exploits to vulnerabilities in software such as Java and Flash. Integrated with the Trend Micro Virus Scan Engine, the Advanced Threat Scan Engine employs signature-based, behavior-based, and aggressive heuristic detection. |
| Deep Discovery Malware Pattern | The Deep Discovery Malware Pattern contains information that helps ATP Analyzer identify the latest malware and mixed threat attacks. Trend Micro creates and releases new versions of the pattern several times a week, and any time after the discovery of a particularly damaging virus/malware. |

| Component | Description |
|---|---|
| IntelliTrap Exception Pattern | The IntelliTrap Exception Pattern contains detection routines for safe compressed executable (packed) files to reduce the amount of false positives during IntelliTrap scanning. |
| IntelliTrap Pattern | The IntelliTrap Pattern contains the detection routines for compressed executable (packed) file types that are known to commonly obfuscate malware and other potential threats. |
| Network Content Correlation Pattern | The Network Content Correlation Pattern implements detection rules defined by Trend Micro. |
| Script Analyzer Engine | The Script Analyzer Engine analyzes web page scripts to identify malicious code. |
| Script Analyzer Pattern | The Script Analyzer Pattern is used during analysis of web page scripts to identify malicious code. |
| Spyware/Grayware Pattern | The Spyware/Grayware Pattern identifies unique patterns of bits and bytes that signal the presence of certain types of potentially undesirable files and programs, such as adware and spyware, or other grayware. |
| Virtual Analyzer Sensors | The Virtual Analyzer Sensors are a collection of utilities used to execute and detect malware and to record behavior in Virtual Analyzer. |

## Component Update Settings Tab

The **Component Update Settings** tab allows you to configure automatic updates and the update source.




| Setting | Description |
|---|---|
| Automatic updates | Select **Automatically check for updates** to keep components up-to-date.<br><br>If you enable automatic updates, TippingPoint Advanced Threat Protection Analyzer runs an update everyday. Specify the time the update runs. |

| SETTING | DESCRIPTION |
|---|---|
| Update source | TippingPoint Advanced Threat Protection Analyzer can download components from the Trend Micro ActiveUpdate server or from another source. You may specify another source if TippingPoint Advanced Threat Protection Analyzer is unable to reach the ActiveUpdate server directly.<br><br>If you choose the ActiveUpdate server, verify that TippingPoint Advanced Threat Protection Analyzer has Internet connection.<br><br>If you choose another source, set up the appropriate environment and update resources for this update source. Also ensure that there is a functional connection between TippingPoint Advanced Threat Protection Analyzer and this update source. If you need assistance setting up an update source, contact your support provider. The update source must be specified in URL format. Specify a host name, IPv4 address or IPv6 address using URL format.<br><br>**Note**<br>When the IPv6 address is part of a URL, enclose the address in square brackets ([]).<br><br>Verify that proxy settings are correct if TippingPoint Advanced Threat Protection Analyzer requires a proxy server to connect to its update source. For details, see *Proxy Tab on page 6-15*. |

## Hot Fixes / Patches Tab

Use the **Hot Fixes / Patches** screen to apply hot fixes and patches to TippingPoint Advanced Threat Protection Analyzer. After an official product release, Trend Micro releases system updates to address issues, enhance product performance, or add new features.

**TABLE 6-2. Hot Fixes / Patches**

| SYSTEM UPDATE | DESCRIPTION |
|---|---|
| Hot fix | A hot fix is a workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and are not released to all customers.<br><br>**Note**<br>A new hot fix may include previous hot fixed until Trend Micro releases a patch. |
| Security patch | A security patch focuses on security issues suitable for deployment to all customers. Non-Windows patches commonly include a setup script. |
| Patch | A patch is a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Non-Windows patches commonly include a setup script. |

Your vendor or support provider may contact you when these items become available. Check the Trend Micro website for information on new hot fix and patch releases:

http://downloadcenter.trendmicro.com/

## Applying a Hot Fix / Patch

Please perform these tasks when using TippingPoint Advanced Threat Protection Analyzer in a high availability cluster configuration.

1. Detach the passive primary appliance. For details, see *Detaching the Passive Primary Appliance from the Cluster on page 6-44*

2. On the active primary appliance, perform the tasks as described in the main task section below.

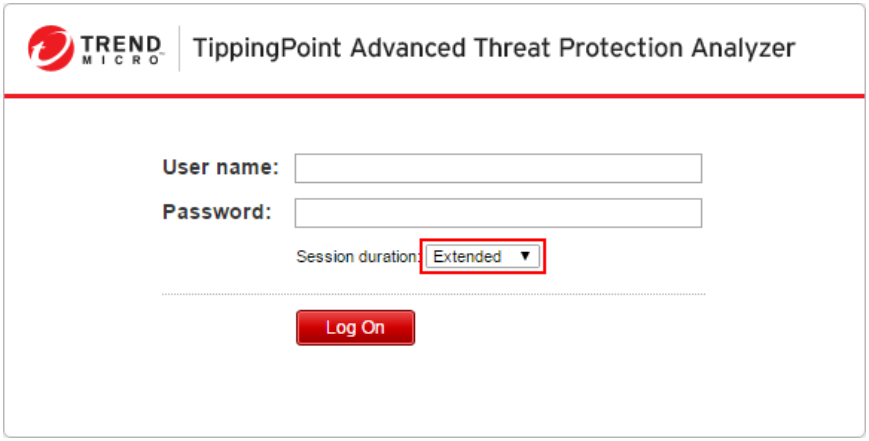
3. On the passive primary appliance, perform the tasks as described in the main task section below.

4. Add the passive primary appliance to the cluster again. For details, see *Adding a Passive Primary Appliance to the Cluster on page 6-42*

## Procedure

1. Obtain the product update file from Trend Micro.
   - If the file is an official patch, download it from the download center.

     http://downloadcenter.trendmicro.com/
   - If the file is a hot fix, send a request to Trend Micro support.
2. On the logon page of the management console, select **Extended** and then log on using a valid user name and password.




3. Go to **Administration** > **Updates** > **Hot Fixes / Patches**.
4. Click **Choose File** or **Browse**, and select the product update file.
5. Click **Install**.

> **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 update is complete.

6. Log on to the management console.
7. Go back to the **Administration** > **Updates** > **Hot Fixes / Patches** screen.
8. Verify that the hot fix / patch displays in the **History** section as the latest update.

## Rolling Back a Hot Fix / Patch

Please perform these tasks when using TippingPoint Advanced Threat Protection Analyzer in a high availability cluster configuration.

1. Detach the passive primary appliance. For details, see *Detaching the Passive Primary Appliance from the Cluster on page 6-44*
2. On the active primary appliance, perform the tasks as described in the main task section below.
3. On the passive primary appliance, perform the tasks as described in the main task section below.
4. Add the passive primary appliance to the cluster again. For details, see *Adding a Passive Primary Appliance to the Cluster on page 6-42*

TippingPoint Advanced Threat Protection Analyzer has a rollback function to undo an update and revert the product to its pre-update state. Use this function if you encounter problems with the product after a particular hot fix / patch is applied.

**Note**

The rollback process automatically restarts TippingPoint Advanced Threat Protection Analyzer, so make sure that all tasks on the management console have been completed before rollback.

**Procedure**

1. Go to **Administration** > **Updates** > **Hot Fixes / Patches**.
2. In the **History** section, click **Roll Back**.

   TippingPoint Advanced Threat Protection Analyzer will automatically restart after the rollback is complete.

3. Log on to the management console.
4. Go back to the **Administration** > **Updates** > **Hot Fixes / Patches** screen.
5. Verify that the hot fix / patch no longer displays in the **History** section.

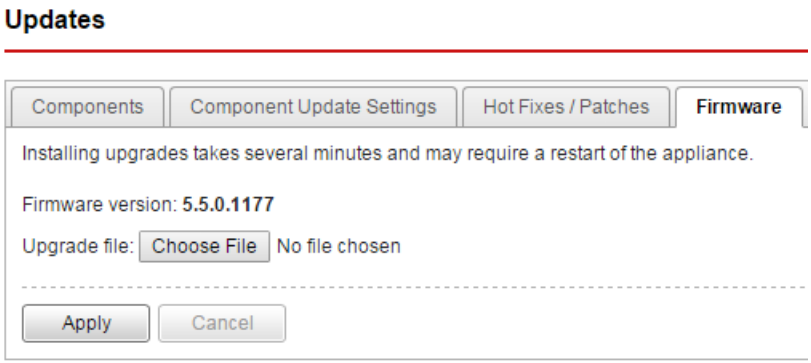
## Firmware Tab

Use the **Firmware** tab to apply an upgrade to TippingPoint Advanced Threat Protection Analyzer. Trend Micro prepares a readme file for each upgrade. Read the accompanying readme file before applying an upgrade for feature information and for special installation instructions.

Please perform these tasks when using TippingPoint Advanced Threat Protection Analyzer in a high availability cluster configuration.

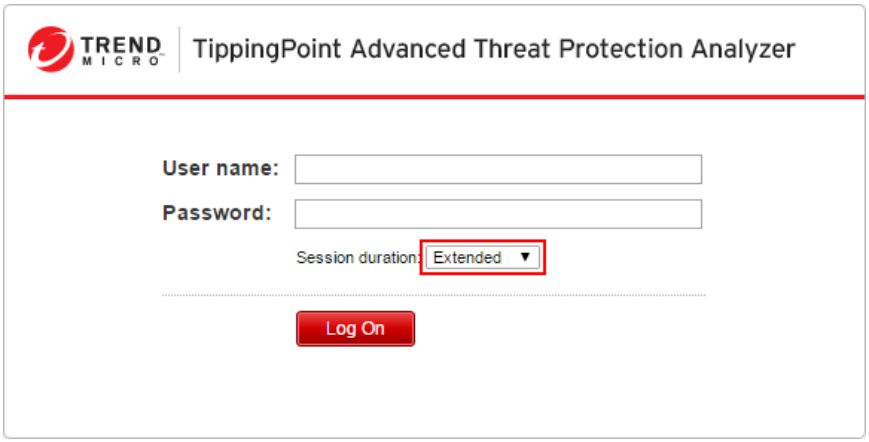
1. Detach the passive primary appliance. For details, see *Detaching the Passive Primary Appliance from the Cluster on page 6-44*
2. On the active primary appliance, perform the tasks as described in the main task section below.
3. On the passive primary appliance, perform the tasks as described in the main task section below.
4. Add the passive primary appliance to the cluster again. For details, see *Adding a Passive Primary Appliance to the Cluster on page 6-42*

Perform the following steps to install the upgrade.




## 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 click the **Firmware** tab.
3. Click **Choose File** or **Browse**, and 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.

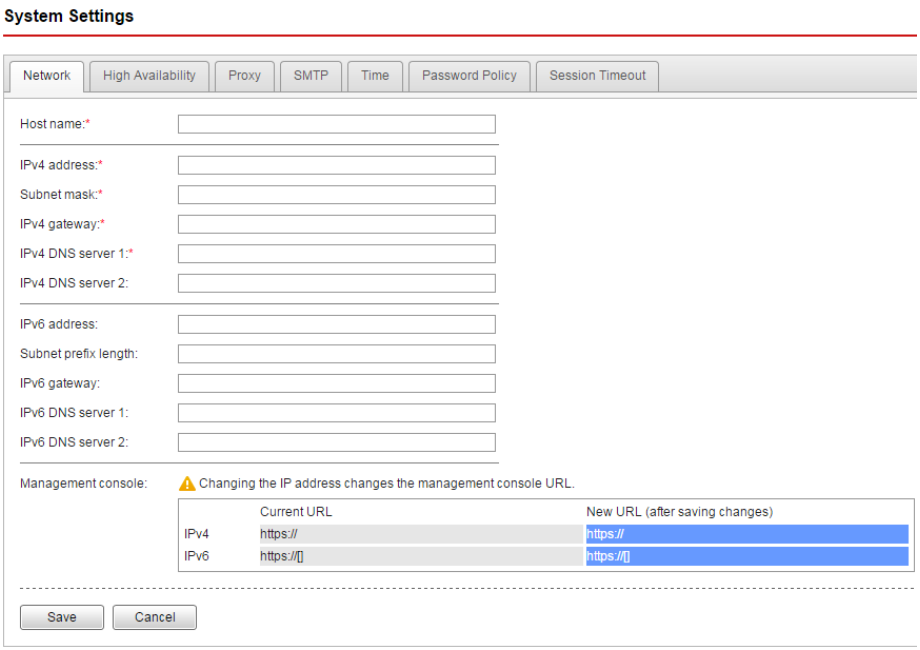
# System Settings

The **System Settings** screen, in **Administration** > **System Settings**, includes the following tabs:


- *Network Tab on page 6-12*
- *High Availability Tab on page 6-13*
- *Proxy Tab on page 6-15*
- *SMTP Tab on page 6-17*
- *Time Tab on page 6-18*
- *Password Policy Tab on page 6-20*
- *Session Timeout Tab on page 6-21*

## 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 *TippingPoint Advanced Threat Protection Analyzer Installation and Deployment Guide*.

---

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 when using TippingPoint Advanced Threat Protection Analyzer in a high availability cluster configuration.

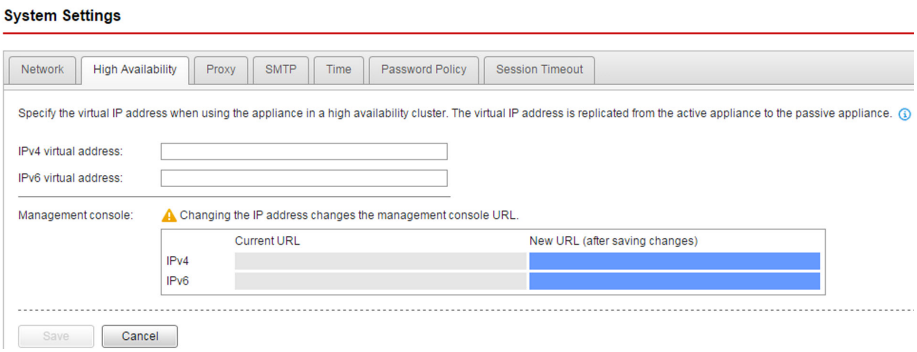
**TABLE 6-3. Configuration Limitations when Using High Availability**

| FIELD | LIMITATION |
|---|---|
| Host name | Cannot be modified |
| IPv4 address | • Must differ from IPv4 virtual address<br>• Must be in the same network segment as IPv4 virtual address |
| IPv6 address | • Must differ from IPv6 virtual address<br>• Must be in the same network segment as IPv6 virtual address<br>• Cannot be deleted if IPv6 virtual address has been configured<br>• Cannot be added or deleted |

## High Availability Tab

Specify the IPv4 and IPv6 virtual addresses when using the appliance in a high availability configuration. The IPv4 and IPv6 virtual addresses are used to provide integrated products with fixed IP addresses for configuration, and also determine the URLs to access the management console.

Trend Micro recommends using the original IP address of the appliance as virtual IP address so that integrated products can continue submitting objects to TippingPoint Advanced Threat Protection Analyzer without any modifications to their settings.



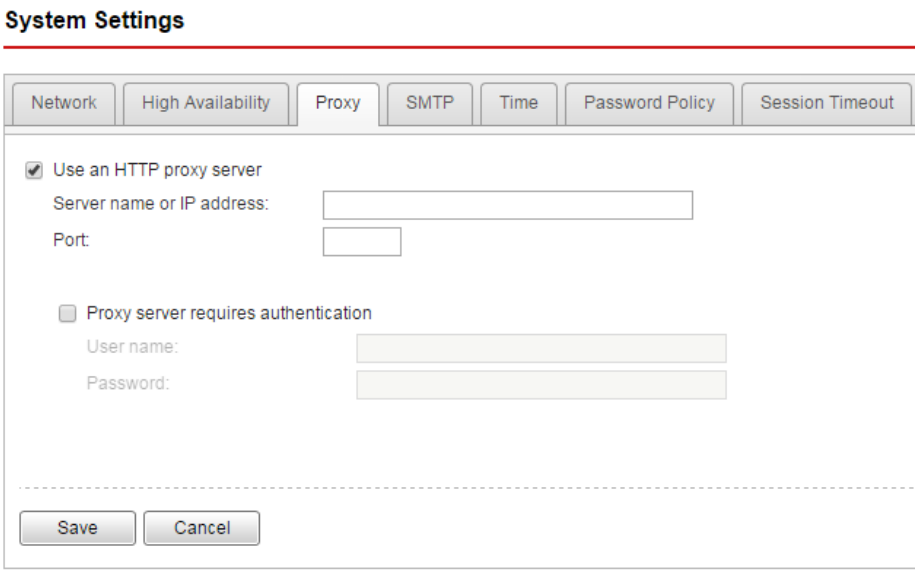

The following table lists configuration limitations when using TippingPoint Advanced Threat Protection Analyzer in a high availability cluster configuration.

**TABLE 6-4. Configuration Limitations when Using High Availability**

| FIELD | LIMITATION |
|---|---|
| IPv4 virtual address | • Cannot be used by another host<br>• Must differ from IPv4 address<br>• Must be in the same network segment as IPv4 address |
| IPv6 virtual address | • Cannot be used by another host<br>• Must differ from IPv6 address<br>• Must be in the same network segment as IPv6 address<br>• Cannot be link-local<br>• Can only be configured when IPv6 address has been configured |

## Proxy Tab

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




Configure the following settings.

**TABLE 6-5. Proxy Tab Tasks**

| TASK | STEPS |
|---|---|
| Use an HTTP proxy server | Select this option to enable proxy settings. |
| Server name or IP address | Type the proxy server host name or IPv4 address, or IPv6 address.<br><br>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. |

| Task | Steps |
|---|---|
| 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:<br>• No authentication<br>• Basic authentication<br>• Digest authentication<br>**Note**<br>TippingPoint Advanced Threat Protection Analyzer product license cannot be validated when connecting to the Internet through proxy server with digest authentication.<br>• NTMLv1 authentication |
| User name | Type the user name used for authentication.<br>**Note**<br>This option is only available if **Proxy server requires authentication** is enabled. |
| Password | Type the password used for authentication.<br>**Note**<br>This option is only available if **Proxy server requires authentication** is enabled. |

## SMTP Tab

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

Configure the following settings.

**TABLE 6-6. SMTP Tab Tasks**

| TASK | STEPS |
|---|---|
| Server address | Type the SMTP server host name, IPv4 address, or IPv6 address.<br><br>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. |

| TASK | STEPS |
|---|---|
| User name | Type the user name used for authentication.<br><br>**Note**<br>This option is only available if **SMTP server requires authentication** is enabled. |
| Password | Type the password used for authentication.<br><br>**Note**<br>This option is only available if **SMTP server requires authentication** is enabled. |

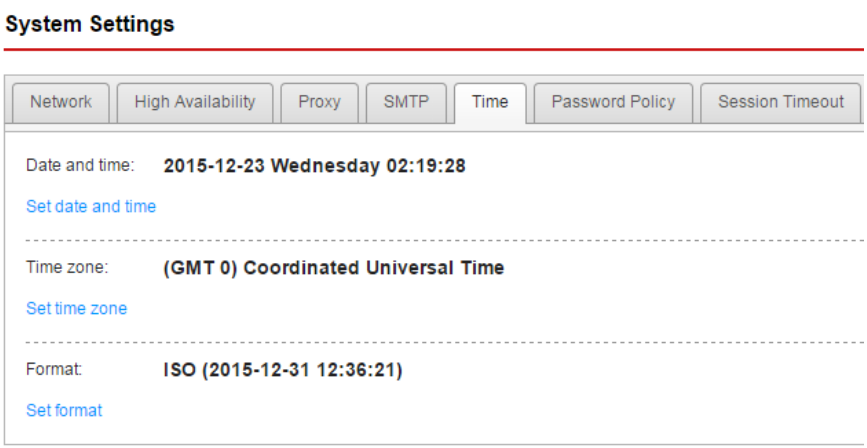
## Time Tab

Configure date and time settings immediately after installation.

### Procedure

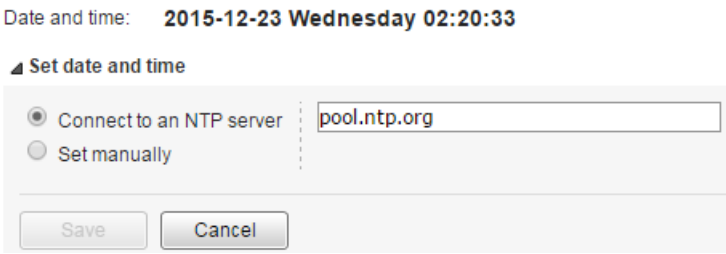
1. Go to **Administration** > **System Settings** and click the **Time** tab.

   The **Time** screen appears.



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

   The settings panel appears.



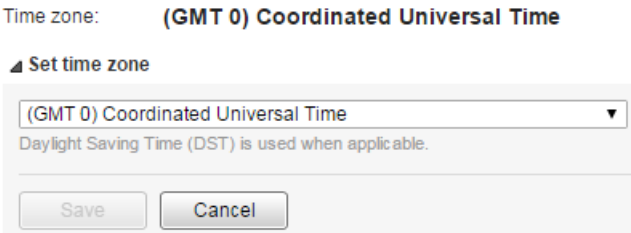

3. Select one of the following methods and configure the applicable settings.

   - 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.




6. Select the applicable time zone.

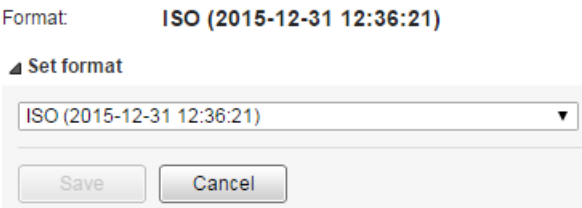
**Note**

Daylight Saving Time (DST) is used when applicable.

7. Click **Save**.

8. Click **Set format**.

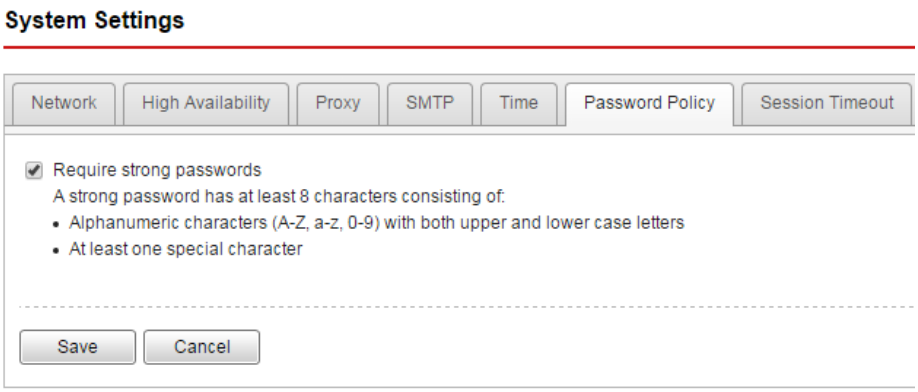
   The settings panel appears.




9. Select the preferred date and time format.
10. Click **Save**.

## Password Policy Tab

Trend Micro recommends requiring strong passwords. Strong passwords usually contain a combination of both uppercase and lowercase letters, numbers, and symbols, and are at least eight characters in length.

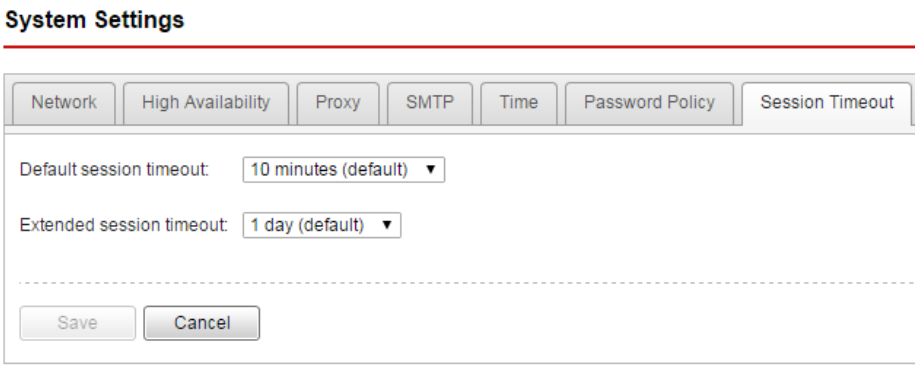



When strong passwords are required, a user submits a new password, and the password policy determines whether the password meets your company's established requirements.

Strict password policies sometimes increase costs to an organization when they force users to select passwords too difficult to remember. Users call the help desk when they forget their passwords, or record passwords and increase their vulnerability to threats. When establishing a password policy balance your need for strong security against the need to make the policy easy for users to follow.

## Session Timeout Tab

At the Login screen of the management console, a user can choose default or extended session timeout.




The default session timeout is 10 minutes and the extended session timeout is one day. You can change these values according to your preference. New values take effect on the next logon.

# Log Settings

TippingPoint Advanced Threat Protection Analyzer maintains system logs that provide summaries of system events, including component updates and appliance restarts. Use the **Log Settings** screen, in **Administration** > **Log Settings**, to configure TippingPoint Advanced Threat Protection Analyzer to send all logs to a syslog server.

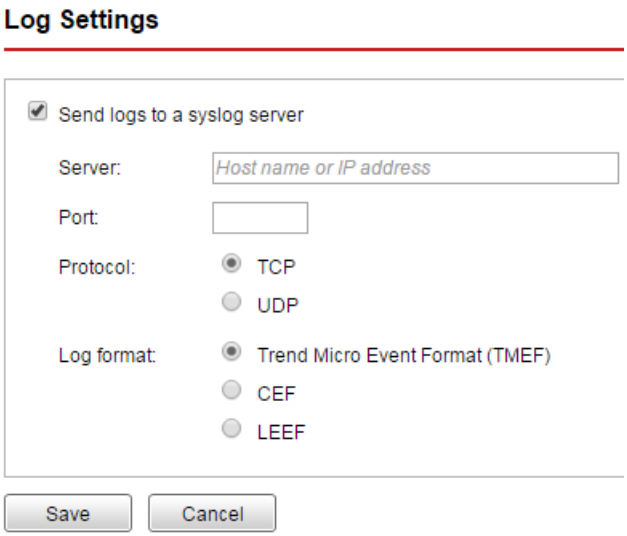
## Configuring Syslog Settings

TippingPoint Advanced Threat Protection Analyzer can forward logs to a syslog server after saving the logs to its database. Only logs saved after enabling this setting are forwarded. Previous logs are excluded.

### Procedure

1. Go to **Administration** > **Log Settings**.

   The **Log Settings** screen appears.




2. Select **Send logs to a syslog server**.
3. Type the host name, IPv4 address, or IPv6 address of the syslog server.
4. Type the port number.

**Note**

Trend Micro recommends using the following default syslog ports:

- **TCP**: 601
- **UDP**: 514

5. Select the protocol to transport log content to the syslog server.
   - TCP
   - UDP
6. Select the format in which event logs are sent to the syslog server.
   - **Trend Micro Event Format (TMEF)**: Trend Micro Event Format (TMEF) is a customized event format developed byTrend Micro and is used by Trend Micro products for reporting event information.
   - **CEF**: Common Event Format (CEF) is an open log management standard developed by HP ArcSight. CEF comprises a standard prefix and a variable extension that is formatted as key-value pairs.
   - **LEEF**: Log Event Extended Format (LEEF) is a customized event format for IBM Security QRadar. LEEF comprises an LEEF header, event attributes, and an optional syslog header.
7. Click **Save**.

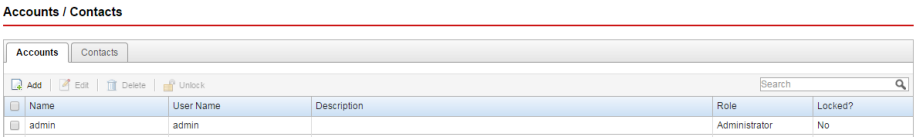
# Accounts / Contacts

The **Accounts / Contacts** screen, in **Administration** > **Accounts / Contacts**, includes the following tabs:

- *Accounts Tab on page 6-24*
- *Contacts Tab on page 6-28*

# Accounts Tab

Use the **Accounts** tab, in **Administration** > **Accounts / Contacts** > **Accounts**, to create and manage user accounts. Users can use these accounts, instead of the default administrator account, to access the management console.




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

This screen includes the following options.

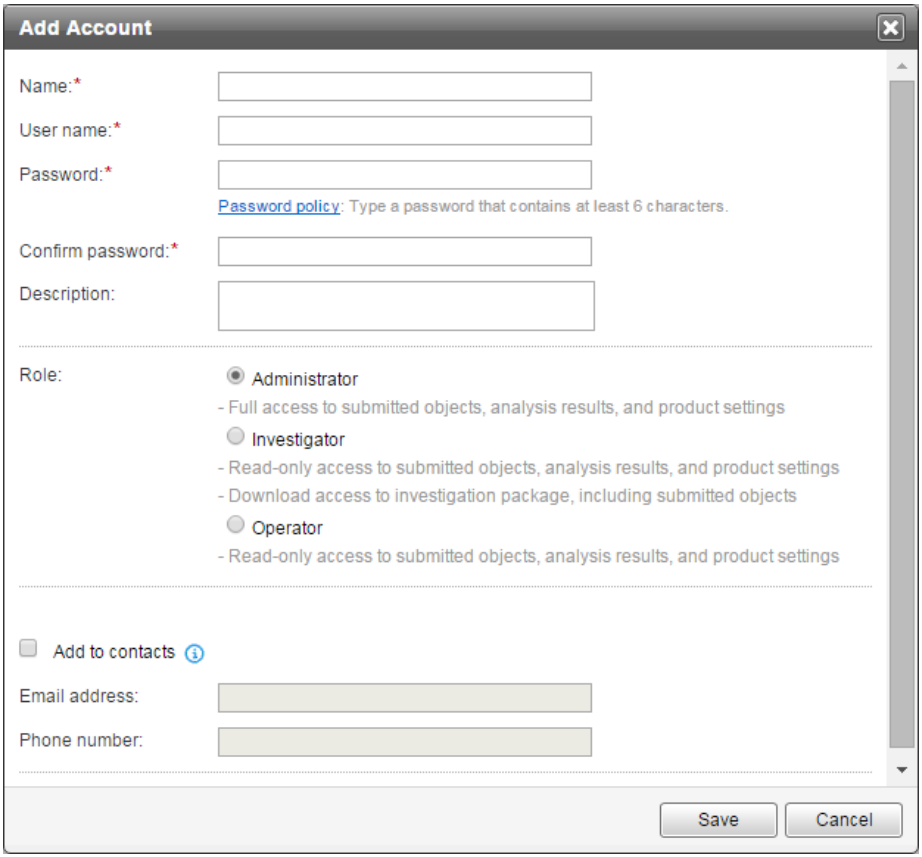
**TABLE 6-7. Accounts Tasks**

| 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 6-26*. |
| 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 6-26*.<br><br>Only one user account can be edited at a time. |
| Delete | Select a user account to delete and then click **Delete**. Only one user account can be deleted at a time. |
| 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.<br><br>Only one user account can be unlocked at a time. |

| Task | Steps |
|---|---|
| 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. |
| 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 add a user account from the **Accounts** screen.




This window includes the following options.

**TABLE 6-8. 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.<br><br>Type a password with at least six characters and then confirm it.<br><br>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.<br><br>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.<br><br>**Tip**<br>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.<br><br>• **Administrator**: Users have full access to submitted objects, analysis results, and product settings<br><br>• **Investigator**: Users have read-only access to submitted objects, analysis results, and product settings, but can download the investigation package, including submitted objects<br><br>• **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. |

# Contacts Tab

Use the **Contacts** tab, in **Administration** > **Accounts / Contacts** > **Contacts**, to maintain a list of contacts who are interested in the data that your logs collect.

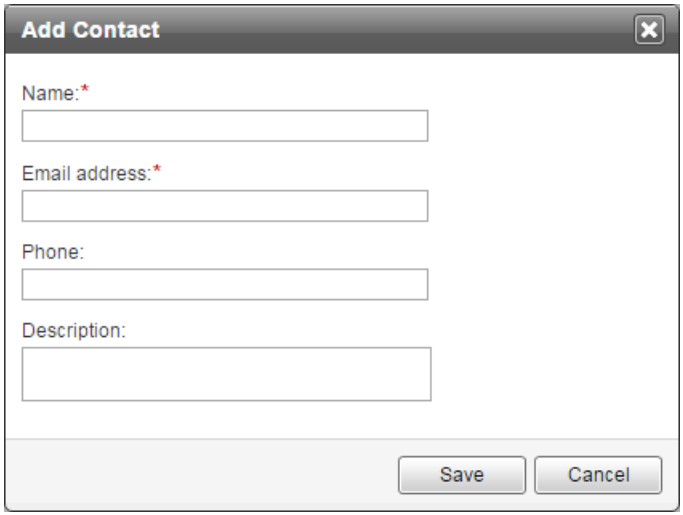
This screen includes the following options.

**TABLE 6-9. Contacts Tasks**

| TASK | STEPS |
|---|---|
| Add Contact | Click **Add Contact** to add a new account. This opens the **Add Contact** window, where you specify contact details. For details, see *Add Contact Window on page 6-28*. |
| Edit | Select a contact and then click **Edit** to edit contact details. This opens the **Edit Contact** window, which contains the same settings as the **Add Contact** window. For details, see *Add Contact Window on page 6-28*.<br><br>Only one contact can be edited at a time. |
| Delete | Select a contact to delete and then click **Delete**. Only one contact can be deleted 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. |
| Records and Pagination Controls | The panel at the bottom of the screen shows the total number of contacts. If all contacts cannot be displayed at the same time, use the pagination controls to view the contacts that are hidden from view. |

## Add Contact Window

The **Add Contact** window appears when you add a contact from the **Contacts** screen.




This window includes the following options.

**TABLE 6-10. Add Contact Window**

| FIELD | DETAILS |
|---|---|
| Name | Type the contact name. |
| Email address | Type the contact's email address. |
| Phone | (Optional) Type the contact's phone number. |
| Description | (Optional) Type a description that does not exceed 40 characters. |

# Audit Logs

TippingPoint Advanced Threat Protection Analyzer maintains audit logs that provide summaries about user access, component updates, setting changes, and other configuration modifications that occurred using the management console.

TippingPoint Advanced Threat Protection Analyzer stores audit logs in the appliance hard drive.

## Querying Audit Logs

**Procedure**

1. Go to **Administration** > **Audit Logs**.
2. Select a type.
   - **All**
   - **System Setting**
   - **Account Logon/Logoff**
   - **System Update**
3. Select a period or specify a custom range using the calendar and sliders.
4. (Optional) Type a keyword in the **User name** field and click the Loupe icon to only display audit logs whose account names contain the keyword.
5. Click **Export all** to export the audit log to a `.csv` file.

# System Maintenance

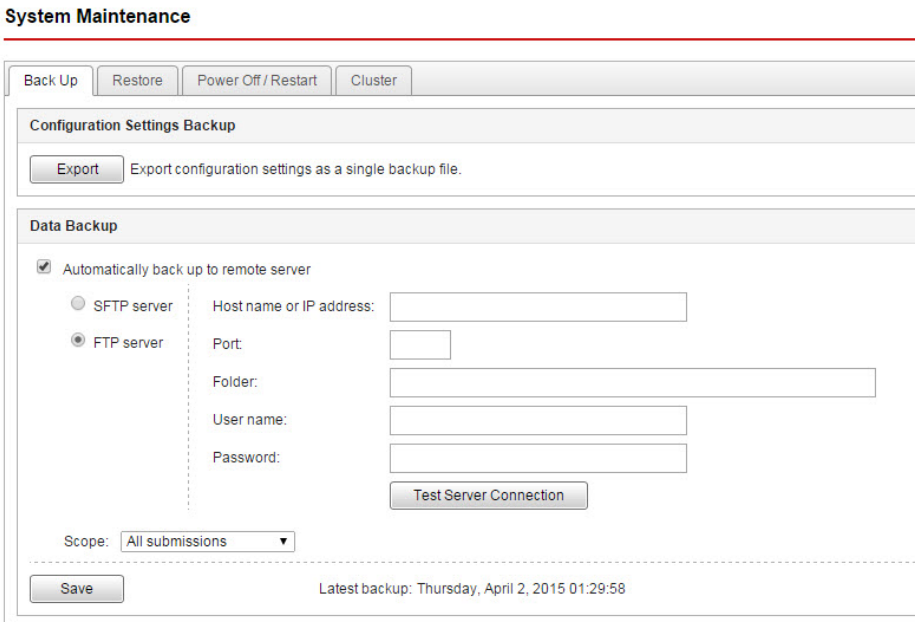
The **System Maintenance** screen, in **Administration** > **System Maintenance**, includes the following tabs:

- *Back Up Tab on page 6-31*
- *Restore Tab on page 6-34*
- *Power Off / Restart Tab on page 6-35*
- *Cluster Tab on page 6-35*

# Back Up Tab

The **Back Up** tab contains settings for the following:

- *Configuration Settings Backup on page 6-31*
- *Data Backup on page 6-32*




## Configuration Settings Backup

TippingPoint Advanced Threat Protection Analyzer can export a backup file of most configuration settings.

To download the configuration settings backup file, click **Export**.

The following table shows the screens and tabs with backed up configuration settings.

**TABLE 6-11. Backed Up Configuration Settings**

| SCREEN | TAB |
|---|---|
| Dashboard | Not applicable (all widgets and settings) |
| Exceptions | Not applicable |
| Sandbox Management | Archive Passwords |
| | Submission Settings |
| | Smart Feedback |
| | Cloud Sandbox |
| Alerts | Rules |
| Report | Schedules |
| | Customization |
| Updates | Component Update Settings |
| System Settings | Proxy |
| | SMTP |
| | Time (time zone and format) |
| | Password Policy |
| | Session Timeout |
| Log Settings | Not applicable |
| Accounts / Contacts | Accounts |
| | Contacts |

## Data Backup

TippingPoint Advanced Threat Protection Analyzer automatically exports submission records, analysis results, and objects to a remote server.

Investigation package data is periodically purged based on available storage space. To ensure availability of the data, Trend Micro recommends backing up the data to an external server. For details, see *Investigation Package Data Retention on page 4-19*.

---

**Procedure**

1. On the **Administration** > **System Maintenance** screen, click the **Back Up** tab.
2. Select **Automatically back up to remote server**.
3. Select the server type.
   - **SFTP server**
   - **FTP server**
4. Type the following information.
   a. **Host name / IP address**: The host name, IPv4 address, or IPv6 address of the backup server.
   b. **Port**: The port number of the backup server.
   c. (Optional) **Folder**: The backup folder path. The default value is the root folder.
   d. **User name**: The user name used for authentication.
   e. **Password**: The password used for authentication.
5. Click **Test Server Connection** to verify the connection to the backup server.
6. Select the scope of the data to back up.
   - **All submissions**
   - **High/Medium/Low risk**
   - **High risk only**
7. Click **Save**.

---

## Restore Tab

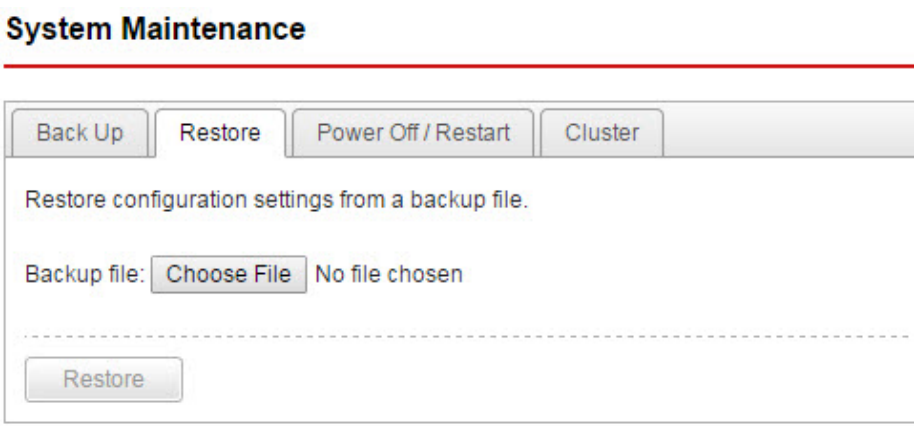
The **Restore** tab restores configuration settings from a backup file.

**Note**

For information on creating a backup file of the configuration settings, see *Back Up Tab on page 6-31*.

**Important**

If the TippingPoint Advanced Threat Protection Analyzer license is not activated, the cloud sandbox setting is not restored.




### Procedure

1. Click **Choose File** or **Browse**.
2. Select the backup file.
3. Click **Restore**.

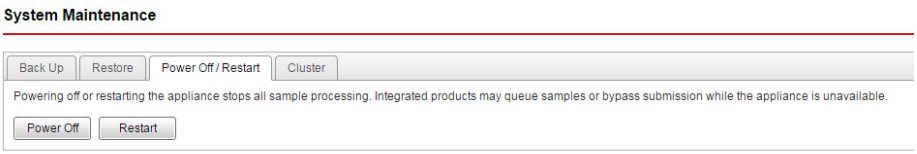
## Power Off / Restart Tab

You can power off or restart the TippingPoint Advanced Threat Protection Analyzer appliance on the management console.

- **Power Off**: All active tasks are stopped, and then the appliance gracefully shuts down.
- **Restart**: All active tasks are stopped, and then the appliance is restarted.

Powering off or restarting the appliance affects the following:

- Virtual Analyzer sample analysis: Integrated products may queue samples or bypass submission while the appliance is unavailable.
- Active configuration tasks initiated by all users: Trend Micro recommends verifying that all active tasks are completed before proceeding.




## 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 6-12. 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. |

For details, see the *TippingPoint Advanced Threat Protection Analyzer Installation and Deployment Guide*.

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

**TABLE 6-13. Cluster Configuration Modes**

| CONFIGURATION MODE | DESCRIPTION |
|---|---|
| **Primary (Active)** | • Management console is fully accessible<br>• Retains all configuration settings |

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

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

## Nodes List

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

The Nodes list contains the following information:

**TABLE 6-14. 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.<br><br>**Note**<br>No data (indicated by a dash) if appliance is passive primary appliance. |

| Column | Description |
|---|---|
| **Details** | Additional details about the operational status of the appliance.<br>• For standalone appliance:<br>  • **Standalone appliance**: The appliance is a standalone appliance.<br>• For passive primary appliance:<br>  • **Fully synced**: The passive primary appliance is fully synced to the active primary appliance.<br>  • **Syncing n%**: The passive primary appliance is syncing settings from the active primary appliance.<br>  • **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.<br>• For secondary appliances:<br>  • **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.<br>  • **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.<br>  • **Invalid API key**: The secondary appliance is configured with an invalid API key. Verify the **Active primary API key** on the secondary appliance.<br>  • **Incompatible software version**: The firmware versions on the active primary appliance and secondary appliance are different. Use the same firmware version on all appliances.<br>  • **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.<br>• For active primary appliance:<br>  • **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 6-43*<br>• For passive primary appliance:<br>  • **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 6-44*<br>  • **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 6-44*<br>• For secondary appliances:<br>  • **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 6-47* |

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 6-15. High Availability Clustering Requirements**

| REQUIREMENT | DESCRIPTION |
|---|---|
| Physical connection | Must be directly connected to each other using eth3 |
| Firmware version | Must have same firmware version |
| Host name | Must be different |
| IP addresses | Must be symmetrical:<br>• If only IPv4 address is configured on active primary appliance, passive primary appliance cannot configure both IPv4 address and IPv6 address.<br>• 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.

### Procedure

1. Perform the installation and deployment tasks as described in the *TippingPoint Advanced Threat Protection Analyzer Installation and Deployment Guide*.

2. Configure the passive primary appliance.

   a. On the management console of the passive primary appliance, go to **Administration** > **System Maintenance** 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 Maintenance** 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, and to modify the host name.

**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 Maintenance** 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 Maintenance** 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 version as the active primary appliance.

To view the appliance firmware version, see the *About on page 6-54* screen.

Update or upgrade the appliance firmware as necessary. For details, see *Updates on page 6-2*.

> **Note**
> If your network has Trend Micro Control Manager, only register the active primary appliance to Control Manager.

### Procedure

1. Perform the installation and deployment tasks as described in the *TippingPoint Advanced Threat Protection Analyzer Installation and Deployment Guide*.
2. Configure the secondary appliance.
   a. On the management console of the secondary appliance, go to **Administration** > **System Maintenance** 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 have a passive primary appliance, 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 *Network Connection Tab on page 4-40*.

**Note**

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

b. Configure the cloud sandbox setting.

For details, see *Cloud Sandbox Tab on page 4-43*.

c. Configure the appliance network settings.

For details, see *Network Tab on page 6-12*.

d. Add accounts.

For details, see *Accounts Tab on page 6-24*.

## 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 Maintenance** 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 6-42*.

**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 Maintenance** 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 6-12*.

   **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.

# Tools

Use the **Tools** screen, in **Administration** > **Tools**, to view and download special tools for TippingPoint Advanced Threat Protection Analyzer.

**Tools**

Downloads require an Internet connection.

| Tool | Description |
|---|---|
| Image Preparation Tool | Before importing an image to Virtual Analyzer, use this tool to check the image for the correct virtual machine settings, supported platforms and required applications.<br>Usage instructions \| Download |
| Manual Submission Tool | Use this tool to remotely submit samples from a local folder to Virtual Analyzer.<br>Usage instructions \| Download |

Each tool displayed on this screen has the following two options:

- **Usage Instructions**: This links to a relevant page in the online help with instructions about how to use the tool.
- **Download**: This links to the relevant page in the download center that has the tool.

## Manual Submission Tool

Use the Manual Submission Tool to remotely submit samples from locations on users' computers to TippingPoint Advanced Threat Protection Analyzer. This feature allows users to submit multiple samples at once, which are added to the **Submissions** queue.

Follow the steps below to download, configure and use the Manual Submission Tool.

**Procedure**

1. Record the following information to use with the Manual Submission Tool.
   a. API key: This is available on the TippingPoint Advanced Threat Protection Analyzer management console, in **Help** > **About**.
   b. TippingPoint Advanced Threat Protection Analyzer IP address: If unsure of the IP address, check the URL used to access the TippingPoint Advanced

Threat Protection Analyzer management console. The IP address is part of the URL.

2. In **Administration** > **Tools**, click the **Download** link for the Manual Submission Tool.

   The Trend Micro **Software Download Center** window appears.

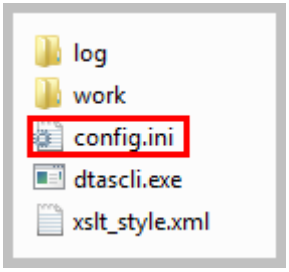
3. Click the download icon next to the latest version.

   A window providing different download options appears.

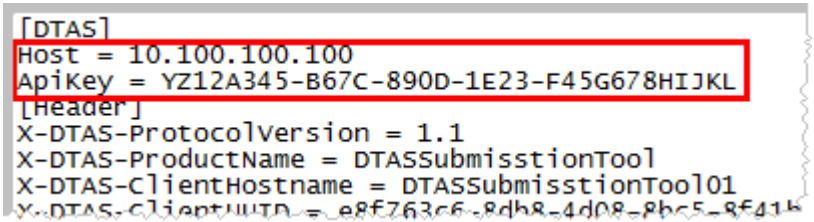
4. Click **Use HTTP Download**.

5. Extract the tool package.

6. In the folder where the tool was extracted, open `config.ini`.




7. Next to `Host`, type the TippingPoint Advanced Threat Protection Analyzer IP address. Next to `ApiKey`, type the TippingPoint Advanced Threat Protection Analyzer API Key. Save `config.ini`.



8. Submit the samples. For details, see *Manually Submitting Objects on page 4-14*.

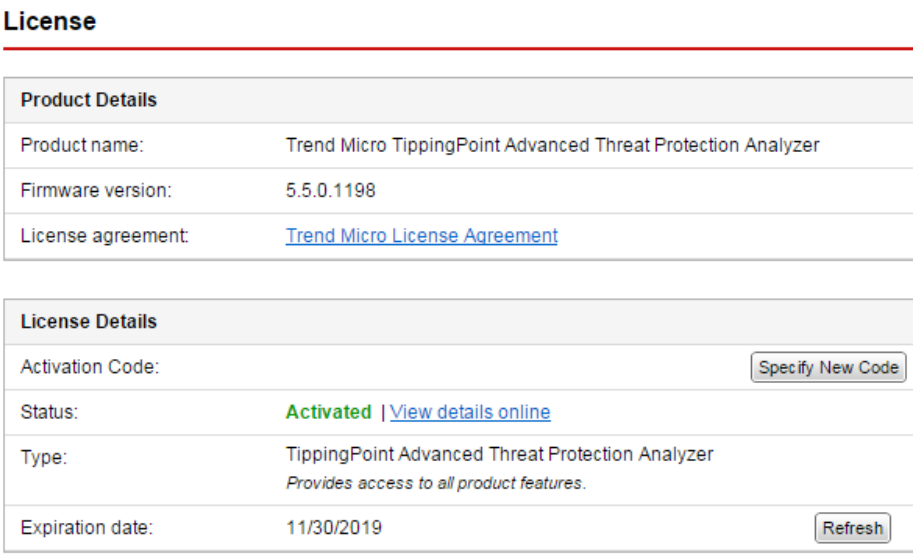
## Image Preparation Tool

Use the Image Preparation Tool before importing an image to Virtual Analyzer. The Image Preparation Tool checks that an image has the correct virtual machine settings, supported platforms and required applications.

For details about the Image Preparation Tool, see the *Virtual Analyzer Image Preparation User's Guide* at http://docs.trendmicro.com/en-us/enterprise/virtual-analyzer-image-preparation.aspx.

# License

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



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 6-16. Product Details**

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

**TABLE 6-17. 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 **Specify New Code**, and type the new Activation Code.<br> <br><br>The **License** screen reappears displaying the number of days left before the product expires. |
| Status | Displays either **Activated**, **Not Activated**, **Evaluation**, or **Expired**.<br>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<br>• 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. |

# About TippingPoint Advanced Threat Protection Analyzer

Use the **About** screen in **Help** > **About** to view the product version, API key, and other product details.

**About**

**Product Information**

**TippingPoint Advanced Threat Protection Analyzer**

| | |
|---|---|
| **Firmware version:** | **5.5.0.1202** |
| **API key:** | |
| **Hardware model:** | **TippingPoint ATP Analyzer 1100 v1** |
| **Service tag:** | **CWBM002** |
| **CPU:** | **Intel(R) Xeon(R) CPU E5-2620 v2 @ 2.10GHz 24 cores** |
| **Installed memory:** | **48 GB** |

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

This software is protected by copyright laws and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Third-party License Attributions

**Note**

The API key is used by Trend Micro products to register and send samples to TippingPoint Advanced Threat Protection Analyzer. For a list of products and supported versions, see *Integration with Trend Micro Products on page 2-6*.

# Chapter 7

# Technical Support

Learn about the following topics:


- *Troubleshooting Resources on page 7-2*
- *Contacting Trend Micro TippingPoint Support on page 7-3*
- *Sending Suspicious Content to Trend Micro on page 7-4*
- *Other Resources on page 7-5*

# Troubleshooting Resources

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

## Using the Support Portal

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

---

**Procedure**

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

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

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

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

---

## 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://www.trendmicro.com/vinfo/us/threat-encyclopedia/#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<br>• International: +1 512 681 8324<br>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

## Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information

- Computer brand, model, and any connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received

# Sending Suspicious Content to Trend Micro

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

## Email Reputation Services

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

https://ers.trendmicro.com

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

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

## File Reputation Services

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

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

Record the case number for tracking purposes.

## Web Reputation Services

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

http://global.sitesafety.trendmicro.com

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

# Other Resources

In addition to solutions and support, there are many other helpful resources available online to help you stay up to date, learn about innovations, and to 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://downloadcenter.trendmicro.com

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

## Service Addresses and Ports

ATP Analyzer accesses several Trend Micro services to obtain information about emerging threats and to manage your existing Trend Micro products. The following table describes each service and provides the required address and port information accessible to the product version in your region.

**Table A-1. Service Addresses and Ports**

| Service | Description | Address and Port |
|---|---|---|
| ActiveUpdate Server | Provides updates for product components, including pattern files. Trend Micro regularly releases component updates through the Trend Micro ActiveUpdate server. | `atpa55-p.activeupdate.trendmicro.com/activeupdate:80`<br>`atpa55-p.activeupdate.trendmicro.com/activeupdate:443` |
| Certified Safe Software Service (CSSS) | Verifies the safety of files. Certified Safe Software Service reduces false positives, and saves computing time and resources. | `gacl.trendmicro.com:443` |
| Cloud Sandbox | A cloud-based service that analyzes possible MacOS threats. | `ddaaas.trendmicro.com:443` |

| Service | Description | Address and Port |
|---|---|---|
| Community File Reputation | Determines the prevalence of detected files. Prevalence is a statistical concept referring to the number of times a file was detected by Trend Micro sensors at a given time. | `atpanalyzer550-en.census.trendmicro.com:80` |
| Customer Licensing Portal | Manages your customer information, subscriptions, and product or service license. | `licenseupdate.trendmicro.com/ollu/license_update.aspx:80` |
| Mobile App Reputation Service (MARS) | Collects data about detected threats in mobile devices. Mobile App Reputation Service is an advanced sandbox environment that analyzes mobile app runtime behavior to detect privacy leaks, repacked mobile apps, third-party advertisement SDKs, vulnerabilities, and app categories. | `rest.mars.trendmicro.com:443` |
| Smart Feedback | Shares anonymous threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. Trend Micro Smart Feedback may include product information such as the product name, ID, and version, as well as detection information including file types, SHA-1 hash values, URLs, IP addresses, and domains. | `atpa550-en.fbs20.trendmicro.com` |
| 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. | `atpan55-threatconnect.trendmicro.com:443` |

| Service | Description | Address and Port |
|---|---|---|
| Web Reputation Services | Tracks the credibility of web domains. Web Reputation Services assigns reputation scores based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis. | `atpa55-en.url.trendmicro.com:80`<br><br>`atpa55-en-wis.trendmicro.com/wis/v1/reason:443` |

# Index


**A**

account management, 6-24
Activation Code, 6-51
administration, 4-36
    archive file passwords, 4-36
Advanced Threat Spam Engine, 5-21, 6-2
alerts, 5-3–5-5, 5-7–5-15, 5-17
    critical alerts, 5-3
    important alerts, 5-4
    informational alerts, 5-5
    notification parameters, 5-7–5-15, 5-17
API key, 6-54
ATSE, 5-21, 6-2
average Virtual Analyzer queue time alert, 5-4

**C**

C&C list, 4-20
components, 6-2
contacting, 7-5
    documentation feedback, 7-5
contact management, 6-28
CPU usage alert, 5-4
critical alerts, 5-3, 5-7
customized alerts and reports, 5-32

**D**

dashboard, 3-7
    dashboard
        tabs, 3-2
    overview, 3-2
    widgets, 3-2, 3-7
Deep Discovery Malware Pattern, 5-21, 6-2
detected message alert, 5-4
detection surge alert, 5-5
disk space alert, 5-4
documentation feedback, 7-5

**E**

email scanning
    archive file passwords, 4-36
exceptions, 4-23

**G**

generated reports, 5-25
getting started tasks, 2-5

**I**

images, 4-28, 4-29
important alerts, 5-4, 5-8–5-15
informational alerts, 5-17
integration with other products, 2-6
IntelliTrap Exception Pattern, 5-21, 6-3
IntelliTrap Pattern, 5-21, 6-3

**L**

license, 6-51
license expiration alert, 5-3
log settings, 6-21
    syslog server, 6-22

**M**

management console, 2-2
    navigation, 2-4
    session duration, 6-21
management console accounts, 6-24
message delivery alert, 5-4

**N**

Network Content Correlation Pattern, 6-3
notification parameters, 5-7

**O**

on-demand reports, 5-26

**P**

preconfiguration console, 2-2
processing surge alert, 5-5
product integration, 2-6

**R**

reports, 5-25, 5-26
    on demand, 5-26
report schedules, 5-28

**S**

sandbox analysis, 4-2
sandbox error alert, 5-3
sandbox images, 4-28, 4-29
sandbox instances, 4-30
sandbox management, 4-25
    archive passwords, 4-35
    images, 4-28
        importing, 4-29
        modifying instances, 4-30
    image status, 4-26
    network connection, 4-40
    Virtual Analyzer status, 4-26
sandbox queue alert, 5-4
Script Analyzer Engine, 6-3
Script Analyzer Pattern, 6-3
service stopped alert, 5-3
session duration (for management console), 2-4
Spyware/Grayware Pattern, 6-3
submissions, 4-2
suspicious objects, 4-20
syslog server, 6-22
system maintenance, 6-30
    back up tab, 6-31
        configuration settings backup, 6-31
        data backup, 6-32
    cluster tab
        primary appliance, 6-47
        remove, 6-47
        secondary appliance, 6-45, 6-47
        test connection, 6-45
    nodes list, 6-38
    restore tab, 6-34
system settings, 6-11
    Network Tab, 6-12
    Password Policy Tab, 6-20
    power off / restart tab, 6-35
    Proxy Tab, 6-15
    Session Timeout Tab, 6-21
    SMTP Tab, 6-17
    Time Tab, 6-18

**T**

tabs in dashboard, 3-3
third-party licenses, 6-54
tools, 6-49
Trend Micro products
    services, A-1

**U**

unreachable relay MTA alert, 5-3
update completed surge, 5-5
update failed alert, 5-4
updates, 6-2
    components, 6-2
    firmware, 6-9
    update settings, 6-4

**V**

Virtual Analyzer, 4-2, 4-36

archive file passwords, 4-36
Virtual Analyzer Sensors, 6-3

## W

watchlist alert, 5-4
widgets, 3-5
add, 3-7

**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: APEM57300/160118