TREND MICRO

5.8

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/en-us/enterprise/tippingpoint-advanced-threat-protection-analyzer.aspx

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

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

Document Part No.: APEM57793/170411

Release Date: April 2017

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

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

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

Evaluate this documentation on the following site:

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

Table of Contents

Preface

Preface vii

Documentation viii

Audience ix

Document Conventions ix

Terminology x

About Trend Micro xii

Chapter 1: Introduction

About TippingPoint Advanced Threat Protection Analyzer 1-2

What's New 1-2

Features and Benefits 1-5

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

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 3-4

Widgets 3-5
Widget Tasks 3-5

Summary Tab 3-8
Threat Types 3-9
Suspicious Objects 3-10
Submissions Over Time 3-11
Virtual Analyzer Summary 3-12

System Status Tab 3-12
Virtual Analyzer Status 3-13
Queued Samples 3-14
Hardware Status 3-15

Chapter 4: Virtual Analyzer

Virtual Analyzer 4-2

Submissions 4-2
Submissions Tasks 4-9
Detailed Information Screen 4-18
Investigation Package 4-20

Suspicious Objects 4-23
Suspicious Objects Tasks 4-24

User-defined Match List 4-26
User-defined Match List Tasks 4-26

Adding Objects to the User-defined Match List 4-27

Exceptions 4-29
Exceptions Tasks 4-29

Sandbox Management 4-33
Status Tab 4-34
Images Tab 4-35
YARA Rules Tab 4-39
Archive Passwords Tab 4-42
Submission Settings Tab 4-44
Network Connection Tab 4-50
Smart Feedback Tab 4-53
Cloud Sandbox Tab 4-53

Submitters 4-54

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 Tab 6-2
Component Update Settings Tab 6-5
Hotfixes / Patches Tab 6-6
Firmware Tab 6-11

Integrated Products/Services 6-12
Log Settings Tab 6-13
Smart Protection Tab 6-16
Deep Discovery Director Tab 6-20

System Settings 6-26
Network Tab 6-27

Proxy Tab 6-28
SMTP Tab 6-30
Time Tab 6-31
SNMP Tab 6-34
Password Policy Tab 6-40
Session Timeout Tab 6-41
Cluster Tab 6-41
High Availability Tab 6-56

Accounts / Contacts 6-57
Accounts Tab 6-57
Contacts Tab 6-61

System Logs 6-62
Querying System Logs 6-63

System Maintenance 6-63
Back Up Tab 6-64
Restore Tab 6-67
Network Services Diagnostics Tab 6-68
Power Off / Restart Tab 6-69
Debug Tab 6-70

Tools 6-72
Virtual Analyzer Image Preparation Tool 6-72
Manual Submission Tool 6-73

License 6-74

About Screen 6-77

Chapter 7: Technical Support

Troubleshooting Resources 7-2
Using the Support Portal 7-2
Threat Encyclopedia 7-2

Contacting Trend Micro 7-3
Speeding Up the Support Call 7-4

Sending Suspicious Content to Trend Micro 7-4
Email Reputation Services 7-4
File Reputation Services 7-5

Web Reputation Services 7-5

Other Resources 7-5
Download Center 7-5
Documentation Feedback 7-6

Appendix A: Service Addresses and Ports

Appendix B: SNMP Object Identifiers

SNMP Query Objects B-2

SNMP Traps B-18

Registration Objects B-22

Index

Index IN-1

Preface

Preface

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

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

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

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

Audience

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

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

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

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

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

Terminology

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

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

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

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to

exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.

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

http://www.trendmicro.com

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

Chapter 1

Introduction

This chapter introduces TippingPoint Advanced Threat Protection Analyzer 5.8 and the new features in this release.

About TippingPoint Advanced Threat Protection Analyzer

TippingPoint Advanced Threat Protection Analyzer is a custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products. TippingPoint Advanced Threat Protection Analyzer supports out-of-the-box integration with Trend Micro email and web security products, and can also be used to augment or centralize the sandbox analysis of other products. The custom sandboxing environments that can be created within TippingPoint Advanced Threat Protection Analyzer precisely match target desktop software configurations — resulting in more accurate detections and fewer false positives.

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

What's New

TABLE 1-1. What's New in TippingPoint Advanced Threat Protection Analyzer 5.8

FEATURE/ENHANCEMENT	DETAILS
Structured Threat Information eXpression (STIX) support	TippingPoint ATP Analyzer adds support for Structured Threat Information eXpression (STIX) files to perform the following functions: • Use of user-defined match list for detection • Export via the WebService API for 3rd party integration

Feature/Enhancement	Details
Enhanced SMTP notification	TippingPoint ATP Analyzer improves the SMTP notifications feature by adding the following enhancements: • Option to specify the port of SMTP server rather than server address only • Default email sender **notifications@atpa.local** • Support for SMTP over SSL/TLS and STARTTLS • Option to test connection to SMTP server
Debug log level settings for troubleshooting	The debug log level settings page enables user to configure debug log level setting for ease in troubleshooting.
Enhanced ActiveUpdate	The enhanced ActiveUpdate includes the following features: • Several new ActiveUpdate components • Option to rollback ActiveUpdate components • Frequency of ActiveUpdate update check increased from every 24 hours to every 15 minutes
Command line arguments for PE samples	TippingPoint ATP Analyzer now provides the option to specify optional command line arguments for PE samples received from integrated products, manual submissions, and support tools.
Enhanced Deep Discovery Director support	Enhanced Deep Discovery Director support provides the following features for TippingPoint ATP Analyzer: • Centralized Virtual Analyzer image deployment • Configuration replication
Enhanced Virtual Analyzer	The internal Virtual Analyzer has been enhanced to include proxy configuration.

Feature/Enhancement	Details
Improved detection capability	TippingPoint ATP Analyzer provides increased protection by improving its detection capabilities. This release supports the following: • Deployment of sandbox images running Windows 10 Threshold 2 (B1511), Windows Server 2012, and Windows Server 2012 R2 operating systems • Support Microsoft Office 2016 application for Office file analysis in sandbox images • New file types (Microsoft Publisher 2016, Microsoft Windows Command Script file, Microsoft Windows Batch file, and Scalable Vector Graphics) for file submission filters • File SHA-256 and vulnerability information in analysis reports • Decrypt password-protected PDF and Microsoft Office files using a password list • Extract files in archive files with multiple compression layers
Enhanced Submission screen	The enhanced **Submission** screen includes the following features: • Improved Advanced filter to provide more search options • A separate **Unsuccessful** tab to display all samples which were not successfully analyzed • Option to customize which columns appear in the Submission screen
Inline migration from TippingPoint ATP Analyzer 5.5 and 5.5 SP1	TippingPoint ATP Analyzer provides users with the option of automatically migrating the settings from 5.5 and 5.5 SP1 to 5.8 using the **Firmware** screen of the management console.
Enhanced credential management	TippingPoint ATP Analyzer uses the same user account and password for the admin account on the management console UI and preconfig screen.

Features and Benefits

TippingPoint Advanced Threat Protection Analyzer includes the following features:

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

Enable Sandboxing as a Centralized Service

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

Custom Sandboxing

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

Broad File Analysis Range

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

YARA Rules

TippingPoint Advanced Threat Protection Analyzer uses YARA rules to identify malware. YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to your environment.

Document Exploit Detection

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

Automatic URL Analysis

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

Detailed Reporting

TippingPoint Advanced Threat Protection Analyzer delivers full analysis results including detailed sample activities and C&C communications via central dashboards and reports.

Alert Notifications

Alert notifications provide immediate intelligence about the state of TippingPoint Advanced Threat Protection Analyzer.

Clustered Deployment

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

Trend Micro Integration

TippingPoint Advanced Threat Protection Analyzer enables out-of-the-box integration to expand the sandboxing capacity Trend Micro email and web security products.

Web Services API and Manual Submission

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

Custom Defense Integration

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

Chapter 2

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™

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:

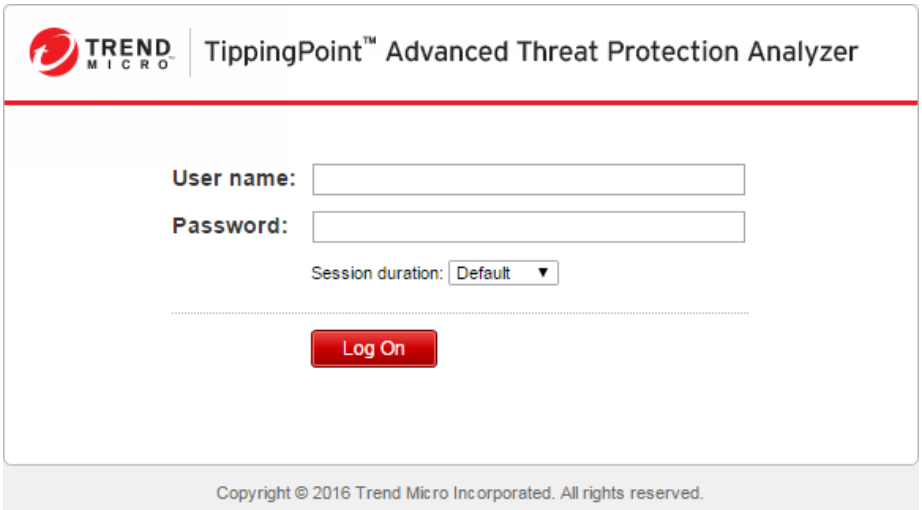


TABLE 2-1. Management Console Logon Options

OPTION	DETAILS
User name	Type the logon credentials (user name and password) for the management console. Use the default administrator logon credentials when logging on for the first time: • User name: `admin` • Password: `Admin1234!` Trend Micro recommends changing the password after logging on to the management console for the first time. Configure user accounts to allow other users to access the management console without using the administrator account. For details, see *Accounts Tab on page 6-57*.
Password	

OPTION	DETAILS
Session duration	Choose how long you would like to be logged on. • **Default**: 10 minutes • **Extended**: 1 day To change these values, navigate to **Administration** > **System Settings** and click the **Session Timeout** tab.
Log On	Click **Log On** to log on to the management console.

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: • Product logo and name: Click to go to the dashboard. For details, see *Dashboard Overview on page 3-2*. • Name of the user currently logged on to the management console. • **Log Off** link: Click to end the current console session and return to the logon screen. • 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 6-74*.
2. Specify the TippingPoint Advanced Threat Protection Analyzer host name and IP address. For details, see *Network Tab on page 6-27*.
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 6-28*.
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 6-31*.
5. Configure SMTP settings to enable sending of notifications through email. For details, see *SMTP Tab on page 6-30*.
6. Import sandbox instances to Virtual Analyzer. For details, see *Importing an Image on page 4-36*.
7. Configure Virtual Analyzer network settings to enable sandbox instances to connect to external destinations. For details, see *Enabling External Connections on page 4-50*.

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 6-41*.

9. Configure supported Trend Micro products for integration with TippingPoint Advanced Threat Protection Analyzer.

10. Adjust Virtual Analyzer resource allocation between all sources by assigning weight and timeout values to all sources that submit objects to TippingPoint Advanced Threat Protection Analyzer for analysis.

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 and investigators 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: • API key. This is available on the TippingPoint Advanced Threat Protection Analyzer management console, in **Help** > **About**. • 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. • 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**. • TippingPoint Advanced Threat Protection Analyzer SSL port 443. This is not configurable. **Important** 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. **Note** Some integrating products require additional configuration to integrate with TippingPoint Advanced Threat Protection Analyzer properly. See the product documentation for details. (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 4-54*.
TippingPoint Advanced Threat Protection for Networks 3.7 or later	
ScanMail for Microsoft Exchange 11.0 or later	
ScanMail for IBM Domino 5.6 SP1 Patch 1 HF4666 or later	
InterScan Messaging Security Virtual Appliance (IMSVA) 8.2 SP2 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 SP2 or later	
OfficeScan 12.0	
Trend Micro Endpoint Sensor 1.6	

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 Email 2.5 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: • API key. This is available on the TippingPoint Advanced Threat Protection Analyzer management console, in **Help** > **About**. • 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. • 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**. • TippingPoint Advanced Threat Protection Analyzer SSL port 443. This is not configurable. **Note** Some of the integrating products require additional configuration to integrate with TippingPoint Advanced Threat Protection Analyzer properly. See the product documentation for details.
TippingPoint Advanced Threat Protection for Networks 3.7 or later	
Standalone Smart Protection Server with the latest patch 2.6 or later	
OfficeScan Integrated Smart Protection Server 10.6 SP2 Patch 1 to OfficeScan Integrated Smart Protection Server 11 SP1	
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 SP3 Patch 2 HF3436 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: • 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. • 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**. • TippingPoint Advanced Threat Protection Analyzer SSL port 443. This is not configurable. • TippingPoint Advanced Threat Protection Analyzer user logon credentials. For details, see *Accounts Tab on page 6-57*. **Important** 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. **Note** 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 SP3 Patch 2 HF3436 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: • 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. • 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**. • TippingPoint Advanced Threat Protection Analyzer SSL port 443. This is not configurable. • TippingPoint Advanced Threat Protection Analyzer user logon credentials. For details, see *Accounts Tab on page 6-57*. **Important** 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. **Note** Some integrating products require additional configuration to integrate with TippingPoint Advanced Threat Protection Analyzer properly. See the product documentation for details.

Chapter 3

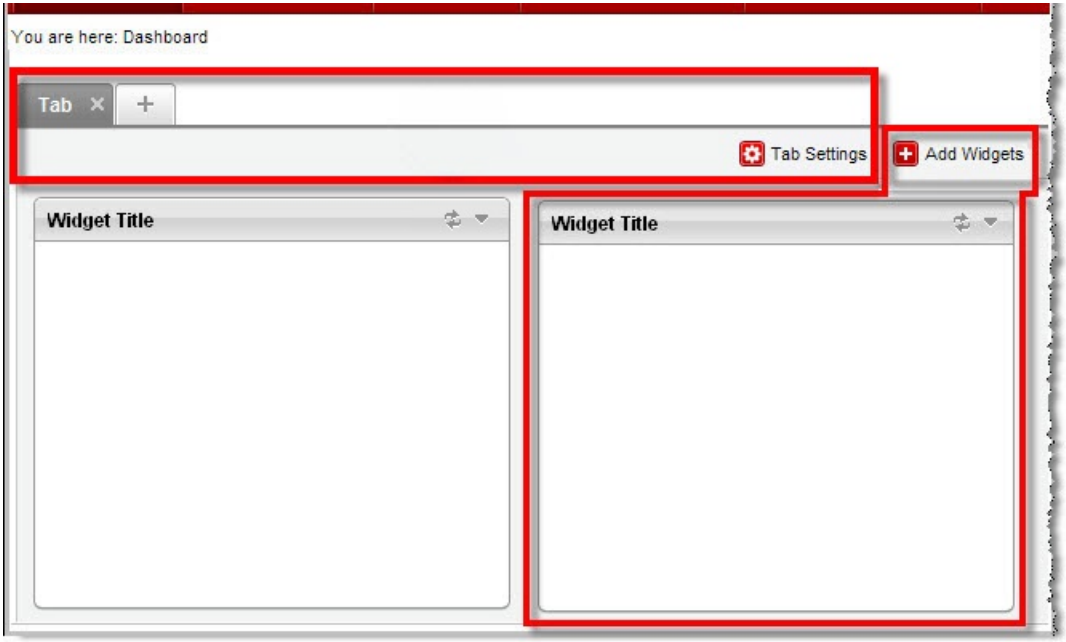
Dashboard

This chapter describes the TippingPoint Advanced Threat Protection Analyzer dashboard.

Dashboard Overview

Monitor your network integrity with the dashboard. Each management console user account has an independent dashboard. Changes made to one user account dashboard do not affect other user account dashboards.

The dashboard consists of the following user interface elements:



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

Note

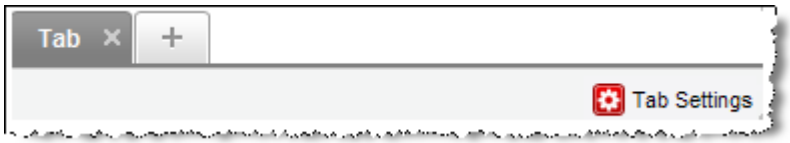
The **Add Widget** button appears with a star when a new widget is available.

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 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 3-4*.
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 click the **plus** icon (+) on top of the dashboard.

This window includes the following options:

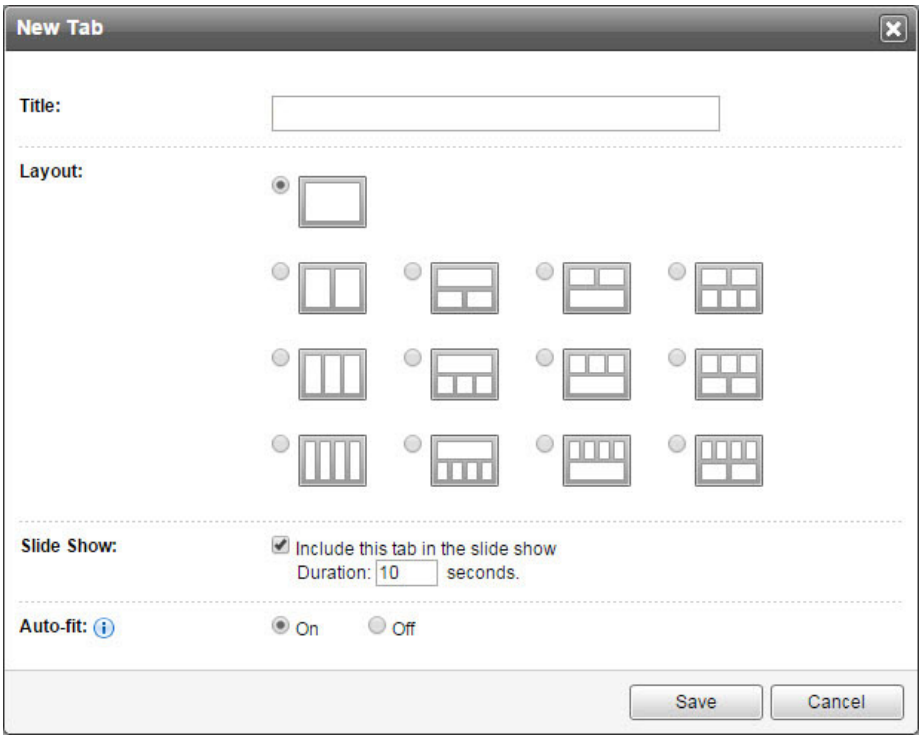


TABLE 3-1. New Tab Tasks

TASK	STEPS
Title	Type the name of the tab.
Layout	Choose from the available layouts.

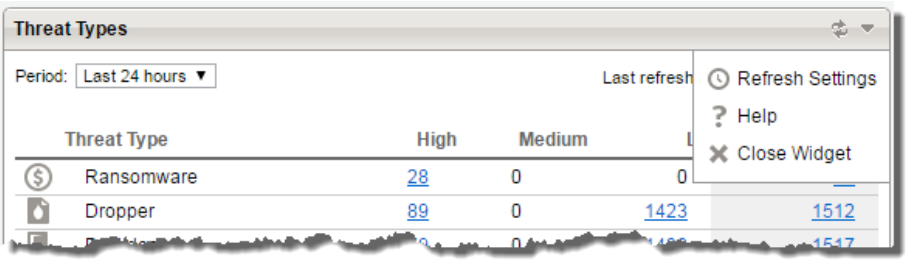
Task	Steps
Slide Show	Select to include the tab in the Dashboard slide show.
Duration	Type the number of seconds to display the tab during the Dashboard slide show.
Auto-fit	Choose **On** or **Off**. This feature works when there is only one widget in a column. Choose **On** to adjust the height of the 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.

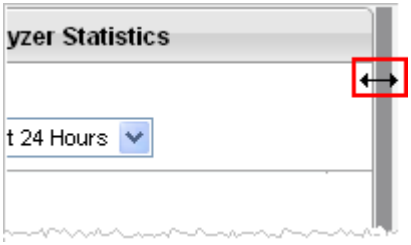
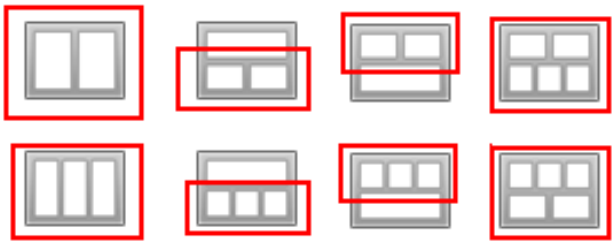
Widget Tasks

All widgets follow a widget framework and offer similar task options.



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*.

Task	Steps
Refresh widget data	Click the refresh icon ( ) to refresh widget data. Click the refresh settings icon ( ) to set the frequency that the widget refreshes or to automatically refresh widget data.
Delete a widget	Click the delete icon ( ) to close the widget. This action removes the widget from the tab that contains it, but not from any other tabs that contain it or from the widget list in the **Add Widgets** screen.
Change period	If available, click the **Period** drop-down menu to select 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 within the same tab	Use drag-and-drop to move the widget to a different location within the tab.

Task	Steps
Resize a widget	Point the cursor to the widget's right edge to resize a 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.  You can resize any widget within a multi-column tab (red squares). These tabs have any of the following layouts. 

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 threats detected by TippingPoint Advanced Threat Protection Analyzer based on type and amount, the volume of suspicious objects discovered during analysis, submissions over time, and the Virtual Analyzer summary.

Threat Types

This widget shows the type, amount, and risk level of threats detected in all submissions during the specified time period.

Threat Types

Period: Last 24 hours ▼ Last refreshed: 01/23/2017 05:53:28 PM

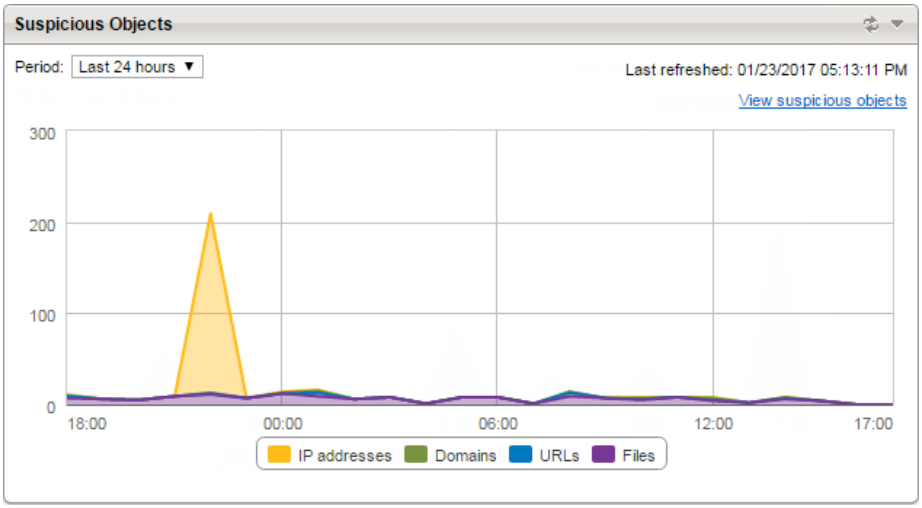
Threat Type	High	Medium	Low	Total
Ransomware	2	0	0	2
Dropper	436	0	12	448
Backdoor	425	0	11	436
Worm	4	0	0	4
Keylogger	2	0	0	2
Bot	1	0	0	1
File infector	1	0	0	1
Exploit	0	0	0	0
Rootkit	0	0	0	0
Downloader	0	0	0	0

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

Click a number under **High**, **Medium**, **Low**, or **Total** to go to the **Submissions** screen and view detailed information.

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 4-23*.

Submissions Over Time

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

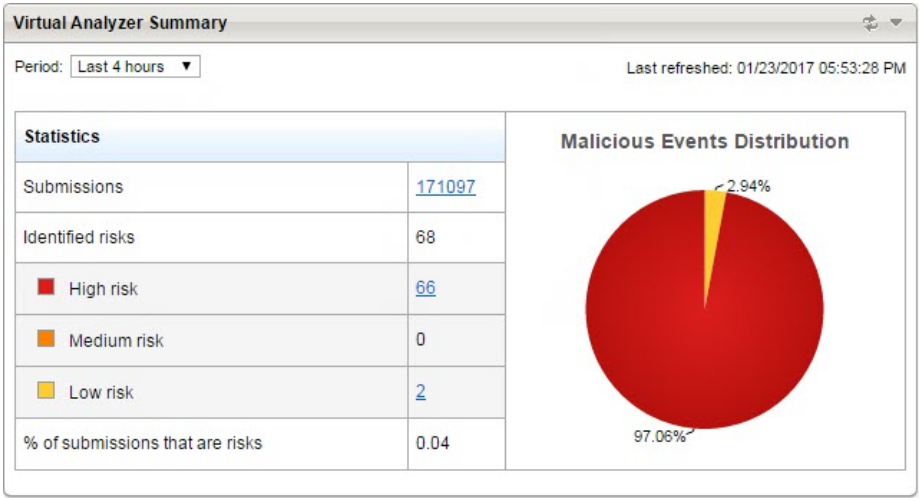
The default period is **Last 24 hours**. Change the period according to your preference.

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.

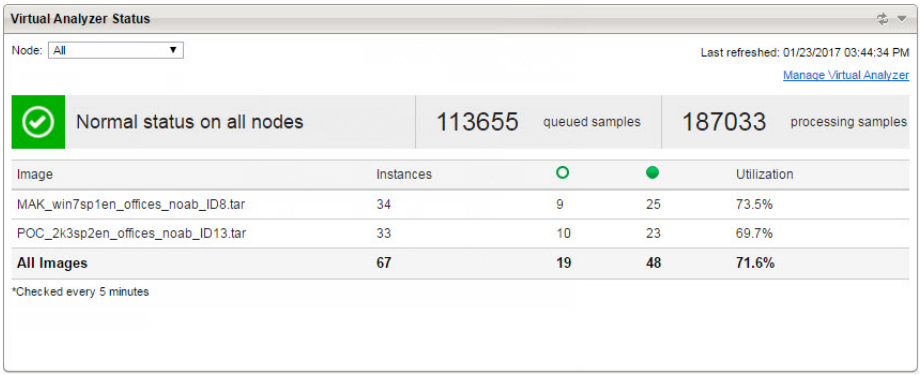
For details, see *Submissions on page 4-2*.

System Status Tab

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

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.



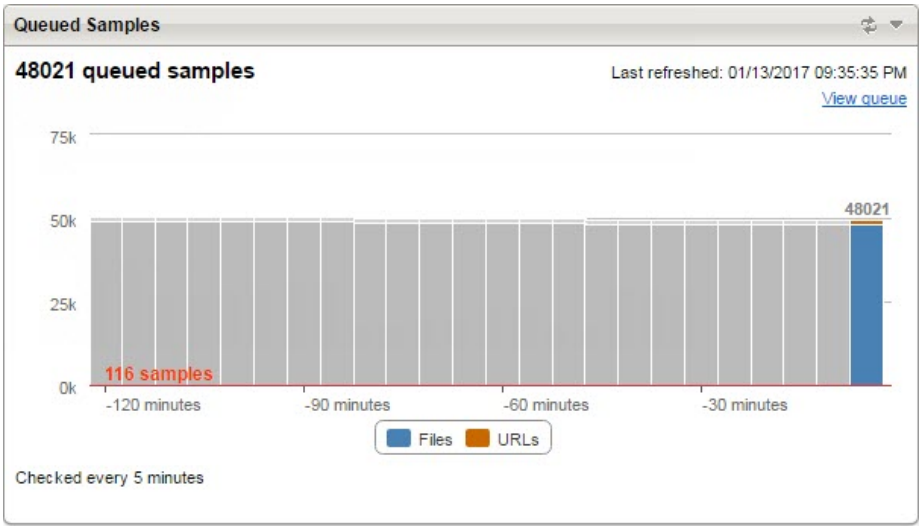
Click **Manage Virtual Analyzer** to go to the **Sandbox Management** screen. For details, see *Sandbox Management on page 4-33*.

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 Settings** and click the **Cluster** tab to view detailed information about the error.

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.

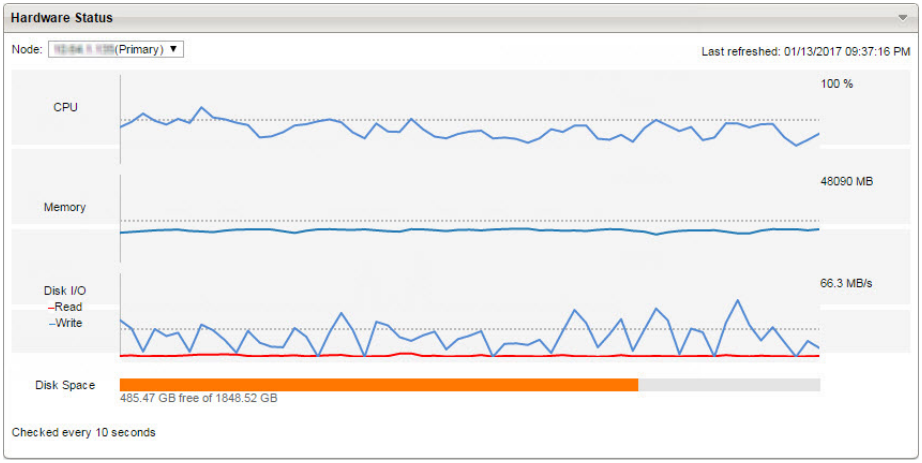


Click **View queue** to go to the **Queued** tab in the **Submissions** screen and view detailed information.

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

Hardware Status

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



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, administrators, and investigators. 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

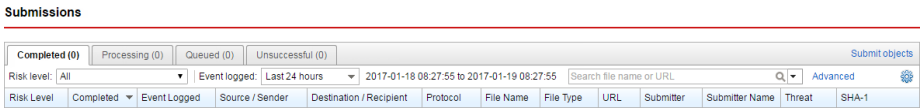
The **Submissions** screen, in **Virtual Analyzer** > **Submissions**, includes a list of samples processed by Virtual Analyzer. Samples are files and URLs submitted

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

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

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

> **Note**
>
> Samples listed in the **Unsuccessful** are not counted by any widget.



Each tab displays a table summarizing basic information about the submitted samples. To customize which columns appear in the table, click the gear icon ( ), select the columns to be displayed in the table, and click **Apply**.

The following table outlines all available columns, and includes columns which are available only on specific tabs.

TABLE 4-1. Submission columns

COLUMN	INFORMATION
Object Information	
Submitted	Date and time when the sample was submitted
File Name	• File name of the sample • File name of the archive / File name of highest risk child object • File name of the archive / File name of any child object if no risk **Note** "NONAMEFL" if file size is 0 or too small for analysis
Submitter	• Name of the Trend Micro product that submitted the sample • "Manual Submission" if manually submitted
Submitter Name	• Host name of the Trend Micro product that submitted the sample • No data (indicated by a dash) if manually submitted
SHA-1	SHA-1 value of the sample
SHA-256	SHA-256 value of the sample This column is available on the **Completed** tab only.
Object Type	File or a URL
Analysis Information	

COLUMN	INFORMATION
Risk Level	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. • **Red icon** ( ): High risk. The object exhibited highly suspicious characteristics that are commonly associated with malware. Examples: • Malware signatures; known exploit code • Disabling of security software agents • Connection to malicious network destinations • Self-replication; infection of other files • Dropping or downloading of executable files by documents • **Yellow icon** ( ): Low risk. The object exhibited mildly suspicious characteristics that are most likely benign. • **Green icon** ( ): No risk. The object did not exhibit suspicious characteristics. • **Gray icon** ( ): Not analyzed For possible reasons why Virtual Analyzer did not analyze a file, see the *Possible Reasons for Analysis Failure* table below. **Note** If several instances processed a sample, 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, the red icon displays. Mouseover the icon for details about the risk level. This column is available on the **Completed** tab only.
Completed	Date and time that sample analysis was completed This column is available on the **Completed** tab only.

COLUMN	INFORMATION
File Type	• File type of the object • File type of the archive / File type of the highest risk child object • File type of the archive / File type of any child object if no risk **Note** "Empty" or "UNKNOWN" if file size is 0 or too small to identify file type for analysis This column is available on the **Completed** tab only.
Threat	Name of threat as detected by Trend Micro pattern files and other components This column is available on the **Completed** tab only.
Threat Types	Type of threat as detected by Trend Micro pattern files and other components This column is available on the **Completed** tab only.
Elapsed Time	The amount of time that has passed since processing started This column is available on the **Processing** tab only.
Processed By	IP address of the node that is processing the object, if TippingPoint Advanced Threat Protection Analyzer is configured in a load-balancing cluster This column is available on the **Completed** and **Processing** tabs only.
Priority	Priority assigned to the sample This column is available on the **Queued** tab only.
Time in Queue	The amount of time that has passed since Virtual Analyzer added the sample to the queue This column is available on the **Queued** tab only.

COLUMN	INFORMATION
Error Reason	Reason for analysis failure This column is available on the **Unsuccessful** tab only.
Event Information	
Event Logged	• For samples submitted by other Trend Micro products, the date and time the product dispatched the sample • For manually submitted samples, the date and time TippingPoint Advanced Threat Protection Analyzer received the sample
Source / Sender	Where the sample originated • IP address for network traffic or email address for email • No data (indicated by a dash) if manually submitted
Destination / Recipient	Where the sample is sent • IP address for network traffic or email address for email • 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 • No data (indicated by a dash) if manually submitted
URL	URL of the sample **Note** TippingPoint Advanced Threat Protection Analyzer may have normalized the URL when submitted using the management console.
Email Subject	Email subject of the sample
Message ID	Message ID of the sample

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
Virtual Analyzer does not support the file format, or the file is empty.	Check the supported file type list in the **Virtual Analyzer** > **Sandbox Management** > **Submission Settings** tab.
The available sandbox images do not support the file format.	Check the sandbox image information in the **Virtual Analyzer** > **Sandbox Management** > **Images** tab.
The URL exceeds the limit of 2083 characters.	Verify that the URL does not exceed 2,083 characters.
The file size exceeds the limit of 60 MB.	Verify that the file size does not exceed 60MB.
Virtual Analyzer does not support the encryption or compression format.	Check the password list in the **Virtual Analyzer** > **Sandbox Management** > **Archive Passwords** tab.
Virtual Analyzer does not support the file format.	Unsupported file type in current sandbox image. Check the sandbox image information in the **Virtual Analyzer** > **Sandbox Management** > **Images** tab.
Virtual Analyzer is unable to access the Internet.	Verify the connection of the management network to the Internet.
An unexpected error has occurred on the cloud sandbox.	Please contact your support provider.
The cloud sandbox did not return an analysis result before the timeout period expired.	Resubmit the object for analysis. If the issue persists, contact your support provider.

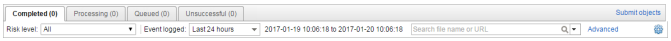
Reason	Action
Unable to establish a connection to the cloud sandbox.	Verify the connection of the management network to the Internet.
The URL is invalid.	Verify that the specified URL is in a valid format.
Extracted file sizes exceeds total limitation	Verify that the total file size of the extracted samples do not exceed the specified limitation.
Archive extracted for analysis. See child files.	Locate the extracted samples.
Virtual Analyzer is unable to analyze the object. The available disk space is insufficient.	Verify that the disk space is sufficient to perform the analysis.
Virtual Analyzer is unable to analyze the object within the timeout period.	Resubmit the object for analysis. If the issue persists, contact your support provider.
An unexpected error has occurred. Please resubmit the sample for analysis. If the issue persists, contact your support provider.	Resubmit the object for analysis. If the issue persists, 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. For details, see *Submitting Objects on page 4-13*. To manually submit multiple files at once, use the Manual Submission Tool. See *Manually Submitting Objects on page 4-15*.
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. For details, see *Detailed Information Screen on page 4-18*.
Prioritize Objects	On the **Queued** tab, select an object and click **Prioritize** to move the object to the top of the queue.

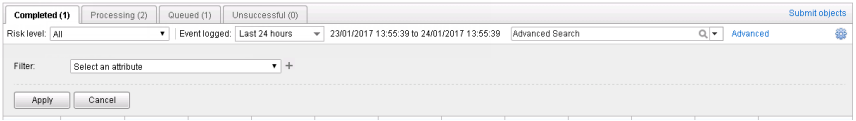
Task	Steps
Data Filters	If there are too many entries in the table, use data filters to limit the entries. Each tab uses a different set of data filters.  Available data filters on the **Completed** tab only: • **Risk level**: Filters by the **Risk Level** column. • **Event logged**: Filters by the **Event Logged** column. All time periods indicate the time used by TippingPoint Advanced Threat Protection Analyzer. If no time period is selected, the default configuration of **Last 24 hours** is used. Available data filters on the **Unsuccessful** tab only: • **Error Reason**: Filters by the **Error Reason** column. • **Submitted**: Filters by the **Submitted** column. All time periods indicate the time used by TippingPoint Advanced Threat Protection Analyzer. If no time period is selected, the default configuration of **Last 24 hours** is used. The following options are available on all tabs: • All tabs contain a search box. Type some characters in the search text box, and then press ENTER. TippingPoint Advanced Threat Protection Analyzer searches only the file names and URLs in the current tab for matches. Performing a search on the **Completed** tab also searches for child file names as well. • The **Advanced** link can limit the entries according to information specified in one or more columns. For details, see *Applying Advanced Filters on page 4-12*.
Customize columns	To customize which columns appear in the table, click the gear icon ( ), select the columns to be displayed in the table, and click **Apply**.
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 **Advanced**.

   The filter bar appears.



2. In the **Filter** drop-down box, select an attribute.

3. Depending on the attribute selected, specify any additional details required by the attribute.

4. To add another attribute, click ➕.

   To remove an attribute, click ✖. You cannot delete the last filter.

5. Click **Apply** to immediately apply the filter to the current table.

   Once applied, the following options are available:

   - **Edit**: Modify the current filter
   - **Clear**: Removes the applied filter
   - **Save**: Saves any changes made to the filter, or saves the filter under a new name

Note

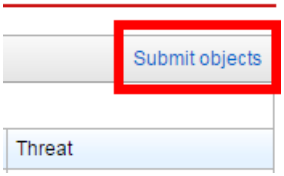
- Filters are saved in the tab where they were created. However, TippingPoint Advanced Threat Protection Analyzer does not allow duplicate filter names, even if they were saved in a different tab.
- Click ▼ on the search text box to view all filters saved for the current tab. Selecting a saved filter immediately applies that filter to the current table.
- Click ✕ to delete a saved filter.

6. Click **Cancel** to discard the current filter.

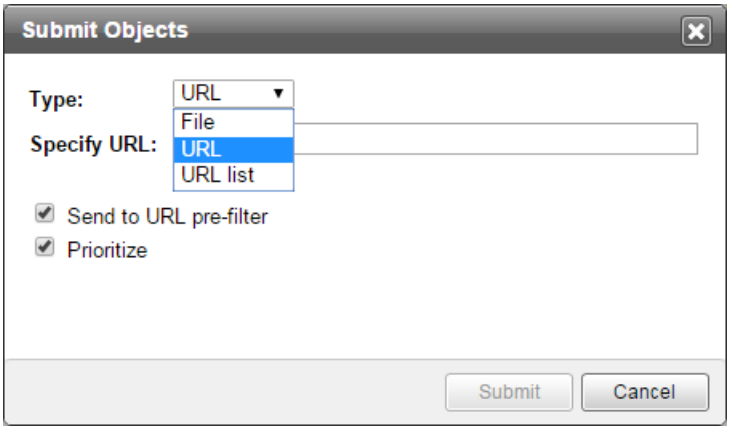
Submitting Objects

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. If the sample to submit is a Portable Executable file, you may specify command line parameters.
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. Files should contain a maximum of 1,000 URLs in the first column. Analysis of 1,000 URLs may take several hours.

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 4-15*.

Manually Submitting Objects

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.

In addition to Microsoft Windows operating systems, the Manual Submission Tool supports the following Linux distributions:

- CentOS/RedHat 5.x (32-bit and 64-bit)
- CentOS/RedHat 6.x (32-bit and 64-bit)
- CentOS/RedHat 7.x (32-bit and 64-bit)
- Ubuntu 12.04 (32-bit)

> **Important**
> `glibc.i686` and `zlib.i686` must be installed on 64-bit Linux distributions.

Manually Submitting Objects in Windows

Procedure

1. If it is not already installed, install the Manual Submission Tool. For details, see *Manual Submission Tool on page 6-73*.
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/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
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: [redacted]
2016-01-27 15:39:04,395 INFO     API Key: [redacted]
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 --url`, `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. If the samples encountered errors during analysis, they appear in the **Unsuccessful** tab.

Manually Submitting Objects in Linux

Procedure

1. If it is not already installed, install the Manual Submission Tool. For details, see *Manual Submission Tool on page 6-73*.
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. Open the terminal, and change the directory (`cd`) to the tool package folder.
4. Execute `chmod +x dtascli`.
5. Depending on the type of object you want to upload, do one of the following:

   Tip

   Execute `./dtascli` for help.

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

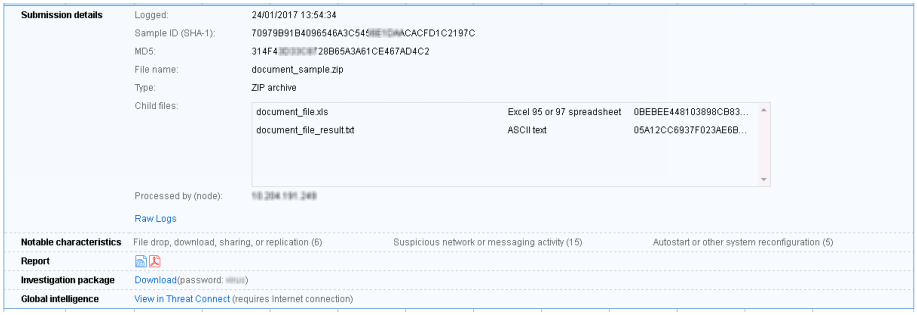
     After executing `./dtascli -u`, `terminal` shows all of the files that were uploaded from the `work/indir` folder.
   - **URL list**: Execute `./dtascli. -u --url` to upload the file `url.txt` in the `work/indir` folder to Virtual Analyzer.

     After executing `./dtascli -u --url`, `terminal` shows all of the files that were uploaded from the `work/indir` folder.
6. 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. If the samples encountered errors during analysis, they appear in the **Unsuccessful** 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, File name, and Type) extracted from the raw logs	Basic data fields (such as Logged, URL, Source IP and port, and Destination IP and port) extracted from the raw logs **Note** TippingPoint Advanced Threat Protection Analyzer may have normalized the URL.
	• Sample ID (SHA-1) • Child files, if available, contained in or generated from the submitted sample • The IP address of the node that processed the sample • The **Raw Logs** link shows all the data fields in the raw logs	

Notable characteristics	• The categories of notable characteristics that the sample exhibits, which can be any or all of the following:
	  • Anti-security, self-preservation
	  • Autostart or other system reconfiguration
	  • Deception, 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
	• 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: • Logged • Protocol • Direction • Source IP • Source Host Name • Destination IP • Destination Host Name	
Report	The PDF icon ( ) links to a downloadable PDF report and the HTML icon ( ) links to an interactive HTML report. **Note** 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. For details, see *Investigation Package on page 4-20*.	
Global intelligence	**View in Threat Connect** is a link that opens Trend Micro Threat Connect 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\SHA1.ioc`	Contains technical characteristics that identify attacker's tactics, techniques and procedures 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.

Path within the Investigation Package	Description
`\common`	Contains files that are common amongst all of the samples.
`\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.
`\%SHA1%\%imageID%\extrainfo`	Contains files related to the sandbox image that analyzed the object.
`\%SHA1%\%imageID%\extrainfo \extra_info.xml`	Contains additional details about the sandbox image that analyzed the object.
`\%SHA1%\%imageID%\strings`	Contains files related to the sandbox image that analyzed the object.
`\%SHA1%\%imageID%\strings\ %SHA1%.string`	Contains string dump retrieved from the object during the analysis in the sandbox image.
`\%SHA1%.ioc`	The IOC file.
`\%SHA1%_ioc.stix`	The STIX IOC file.
`\%SHA1%_so.stix`	The STIX SO file.

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 6-66*.

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.

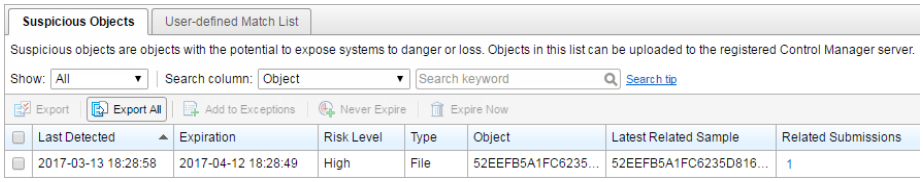
After about 62 days, the 4 TB disk from TippingPoint Advanced Threat Protection Analyzer 1100 is filled and the investigation package data is purged.

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
Risk Level	If the suspicious object is: • **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. • **URL**: The risk level that shows is **High** or **Medium** • **File**: The risk level that shows is always **High** Risk level descriptions: • **High**: Known malicious or involved in high-risk connections • **Medium**: IP address/domain/URL is unknown to reputation service
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. Clicking the number opens the **Submissions** screen with the SHA-1 hash value as the search criteria.

Suspicious Objects Tasks

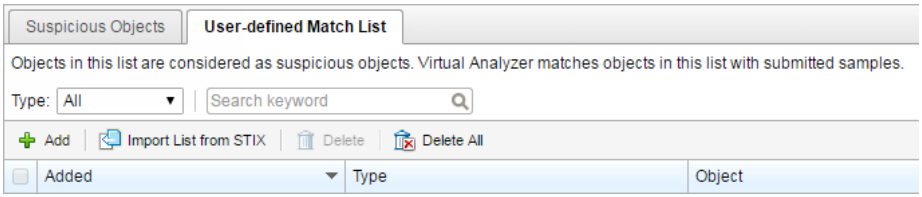
The following table lists all the **Suspicious Objects** tab tasks:

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. 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: • Select an object type in the **Show** drop-down box. • 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.

User-defined Match List

The **User-defined Match List** tab allows users to manually add suspicious objects to TippingPoint Advanced Threat Protection Analyzer using the Structured Threat Information eXpression (STIX) format.



The following columns show information about objects added to the **User-defined Match List**:

TABLE 4-7. User-defined Match List Columns

COLUMN NAME	INFORMATION
Added	Date and time when the suspicious object was added
Type	IP address, Domain, URL, or File
Object	The IP address, domain, URL, or SHA-1 hash value of the file Click **Edit** to modify the displayed value.

User-defined Match List Tasks

The following table lists all the **User-defined Match List** tab tasks:

TABLE 4-8. User-defined Match List Tasks

TASK	STEPS
Add	Click to add a new custom object. For details, see. *Adding Objects to the User-defined Match List on page 4-27*.
Import List from STIX	Click to add objects using a STIX file in the XML format. **Note** • TippingPoint Advanced Threat Protection Analyzer can import STIX files formatted using the 1.2, 1.1, and 1.0 version specifications. • The STIX file can include multiple objects, but only the IP addresses, domains, URLs, and SHA-1 hash values specified in the STIX file will be imported.
Delete/Delete All	Select one or several objects and then click **Delete** to delete the objects. Click **Delete All** to delete all the objects.

Adding Objects to the User-defined Match List

Procedure

1. Click **Add** to add an object.

   The **Add Object** window appears.

2. Select an object type:

   - **IP address**: type the IP address or a hyphenated range.

     Note

     TippingPoint Advanced Threat Protection Analyzer supports both IPv4 and IPv6 formats.

- **Domain**: type a domain name.

  Note

  Wildcards are only allowed in a prefix, and must be connected with a ". " symbol. Use only one wildcard per domain. For example, *.com will match abc.com or test.com.

- **URL**: type the URL.

  Note

  TippingPoint Advanced Threat Protection Analyzer supports both HTTP and HTTPS.

  Wildcards are only allowed in a prefix. Wildcards used in the domain part of an URL must be connected with a ". " symbol. Use only one wildcard per URL. For example, http://*.com will match abc.com or test.com.

  A wildcard can match any part of the URL's URI part. For example, http://abc.com/*abc will match http://abcd.com/test.abc.

- **File**: type the SHA-1 hash value of the file.

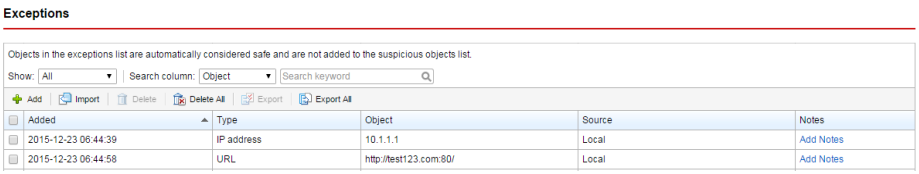
3. Click **Add**.

   Note

   The **User-defined Match List** supports a maximum of 20,000 objects.

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 4-9. Exceptions Columns

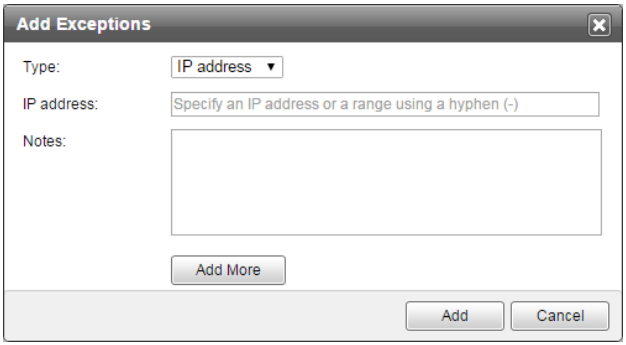
COLUMN NAME	INFORMATION
Added	Date and time Virtual Analyzer added the object to the **Exceptions** tab
Type	IP address, domain, URL, or file
Object	The IP address, domain, URL, or SHA-1 hash value of the file
Source	The source (local or Control Manager) that added the exception
Notes	Notes for the object.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

Exceptions Tasks

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

TABLE 4-10. Exceptions Tasks

TASK	STEPS
Add	1. Click **Add** to add an object.

Task	Steps
	The **Add Exceptions** window appears.  2. Specify the **IP address**, **Domain**, **URL**, or **File** exception criteria. • For IP addresses, select **IP address** for the type and then type the IP address or a hyphenated range. • For domains, select **Domain** for the type and then type the domain. **Note** 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. • For URLs, select **URL** for the type and then type the URL.

Task	Steps
	Note • 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. • 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. • TippingPoint Advanced Threat Protection Analyzer accepts both HTTP and HTTPS URLS. • For files, select **File** for the type and type the SHA-1 hash value. • **Notes**: Type some notes for the object. • **Add More**: Click this button to add more objects. Select an object type, type the object in next field, type some notes, and then click **Add to List**. 3. (Optional) Type some notes for the object. 4. Click **Add More** to add more objects. a. Specify the **IP address**, **Domain**, **URL**, or **File** exception criteria. b. Click **Add to List**. 5. Click **Add** when you have defined all the objects that you wish to add. **Note** TippingPoint Advanced Threat Protection Analyzer supports the addition of up to 25,000 exceptions.
Import	Click **Import** to add objects from a properly-formatted CSV file. In the new window that opens:

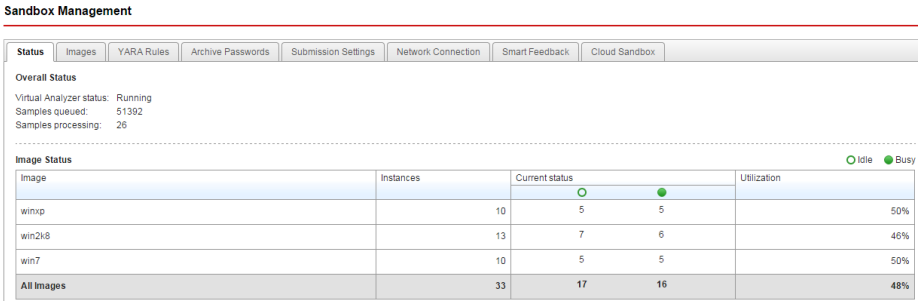
Task	Steps
	• If you are importing exceptions for the first time, click **Download sample CSV**, save and populate the CSV file with objects (see the instructions in the CSV file), browse and then select the CSV file. • If you have imported exceptions previously, save another copy of the CSV file, populate it with new objects, browse and then select the CSV file. **Important** • Importing replaces all entries in the current exception list with the entries in the CSV file. To keep a copy of the current exception list, export the list before starting the import process. • A CSV file can import a maximum of 25,000 exceptions. • If the appliance is integrated with Control Manager, TippingPoint Advanced Threat Protection Analyzer also uses any exception added in Control Manager. Control Manager can also store a maximum of 25,000 exceptions.
Delete/Delete All	Select one or several objects to remove and then click **Delete**. 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. 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: • Select an object type in the **Show** drop-down box. • 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

TASK	STEPS
	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 4-34*
- *Images Tab on page 4-35*
- *YARA Tab on page 4-39*
- *Archive Passwords Tab on page 4-42*
- *Submission Settings Tab on page 4-44*
- *Network Connection Tab on page 4-50*
- *Smart Feedback Tab on page 4-53*
- *Cloud Sandbox Tab on page 4-53*



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 4-11. Virtual Analyzer Statuses

STATUS	DESCRIPTION
Not initialized	Virtual Analyzer has not been initialized.
No images	No images have been imported into Virtual Analyzer.
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.
Configuring...	Virtual Analyzer is configuring sandbox settings.
Starting...	Virtual Analyzer is starting all sandbox instances.
Running	Virtual Analyzer is analyzing or ready to analyze samples.
Stopping...	Virtual Analyzer is stopping all sandbox instances.
Unrecoverable error	Virtual Analyzer is unable to recover from an error. Contact your support provider for troubleshooting assistance.

STATUS	DESCRIPTION
Deploying images from Deep Discovery Director...	Virtual Analyzer is deploying images from Deep Discovery Director.

- 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 4-12. 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

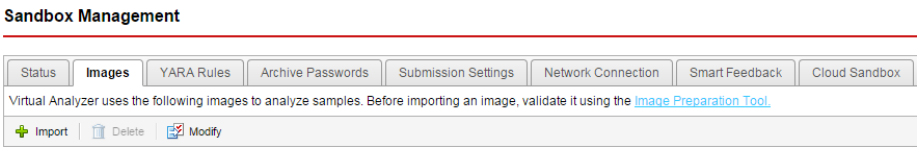
Images Tab

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.

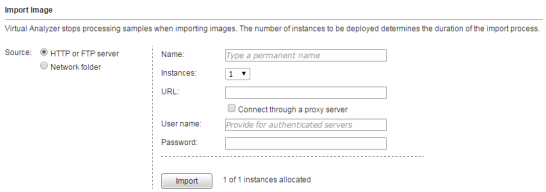
Procedure

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.

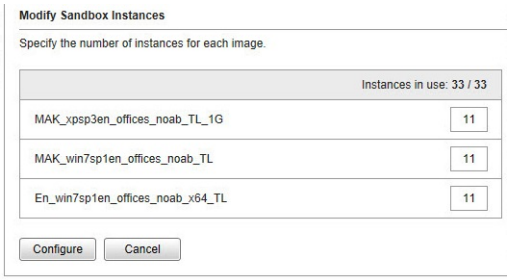
Procedure

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

   The **Images** screen appears.

2. Click **Modify**.

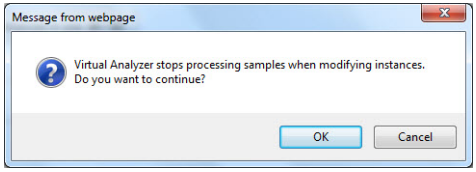
   The **Modify Sandbox Instances** screen appears.



3. Modify the instances allocated to any image.

4. Click **Configure**.

   Virtual Analyzer displays a confirmation message.



5. Click **OK**.

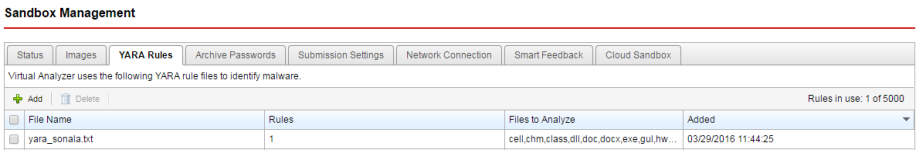
   Virtual Analyzer configures the sandbox instances. Please wait for the process to finish before navigating away from the screen.

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 4-13. YARA Rules columns

COLUMN NAME	INFORMATION
File name	Name of the YARA rule file
Rules	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 4-14. 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 4-42*.
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

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 4-15. 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.
weight	Optional part that must be between 1 and 10 that determines the risk level if rule conditions are met: • 1 to 9 = Low risk • 10 = High risk **Note** The weight value does not correspond to the risk level assigned by TippingPoint Advanced Threat Protection Analyzer.
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.

PART	USAGE
$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 4-40*.

Archive Passwords Tab

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

TippingPoint Advanced Threat Protection Analyzer uses user-specified passwords to extract files or open password-protected documents. For better performance, list commonly used passwords first.

TippingPoint Advanced Threat Protection Analyzer supports the following password-protected archive file types:

- `7z`
- `zip`
- `tar`
- `arj`

TippingPoint Advanced Threat Protection Analyzer supports the following password-protected document file types:

- `doc`
- `docx`
- `pdf`
- `ppt`
- `pptx`
- `xls`
- `xlsx`

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

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 4-16. Virtual Analyzer File Types

DISPLAYED FILE TYPE	FULL FILE TYPE	EXAMPLE FILE EXTENSIONS
bat	Microsoft™ Windows™ batch file	`.bat`
cmd	Microsoft™ Windows™ command script file	`.cmd`
cell	Hancom™ Hancell spreadsheet	`.cell`
chm	Compiled HTML (CHM) help file	`.chm`
class	Java™ Class file	`.class` `.cla`

dll	AMD™ 64-bit DLL file
	Microsoft™ Windows™ 16-bit DLL file
	Microsoft™ Windows™ 32-bit DLL file
		`.dll`
		`.ocx`
		`.drv`

doc	Microsoft™ Word™ 1.0 document Microsoft™ Word™ 2.0 document	`.doc` `.dot`

docx	Microsoft™ Office Word™ (2007 or later) document
	Microsoft™ Office Word™ (2007 or later) macro-enabled document
		`.docx`
		`.dotx`
		`.docm`
		`.dotm`

Displayed File Type	Full File Type	Example File Extensions

exe	AMD™ 64-bit EXE file
	ARJ compressed EXE file
	ASPACK 1.x compressed 32-bit EXE file
	ASPACK 2.x compressed 32-bit EXE file
	DIET DOS EXE file
	GNU UPX compressed EXE file
	IBM™ OS/2 EXE file
	LZEXE DOS EXE file
	LZH compressed EXE file
	LZH compressed EXE file for ZipMail
	MEW 0.5 compressed 32-bit EXE file
	MEW 1.0 compressed 32-bit EXE file
	MEW 1.1 compressed 32-bit EXE file
	Microsoft™ Windows™ 16-bit EXE file
	Microsoft™ Windows™ 32-bit EXE file
	MIPS EXE file
	MSIL Portable executable file
	PEPACK compressed executable
	PKWARE™ PKLITE™ compressed DOS EXE file
	PETITE compressed 32-bit executable file
	PKZIP compressed EXE file
	WWPACK compressed executable file
		`.cpl`
		`.exe`
		`.sys`
		`.crt`
		`.scr`

gul	JungUm™ Global document	`.gul`
hta	HTML Application file	`.hta`

Displayed File Type	Full File Type	Example File Extensions
hwp	Hancom™ Hangul Word Processor (HWP) document	.hwp
hwpx	Hancom™ Hangul Word Processor (2014 or later) (HWPX) document	.hwpx
jar	Java™ Applet Java™ Application **Note** Virtual Analyzer does not support the java library.	.jar
js	JavaScript™ file	.js
jse	JavaScript™ encoded script file	.jse
jtd	JustSystems™ Ichitaro™ document	.jtd
lnk	Microsoft™ Windows™ Shell Binary Link shortcut Microsoft™ Windows™ 95/NT shortcut	.lnk
mov	Apple QuickTime media	.mov
pdf	Adobe™ Portable Document Format (PDF)	.pdf
ppt	Microsoft™ Powerpoint™ presentation	.ppt .pps
pptx	Microsoft™ Office PowerPoint™ (2007 or later) presentation Microsoft™ Office PowerPoint™ (2007 or later) macro-enabled presentation	.pptx .ppsx
ps1	Microsoft™ Windows™ PowerShell script file	.ps1
pub	Microsoft™ Office Publisher™ (2016) file	.pub

Displayed File Type	Full File Type	Example File Extensions
rtf	Microsoft™ Rich Text Format (RTF) document	`.rtf`
svg	Scalable Vector Graphics file	`.svg`
swf	Adobe™ Shockwave™ Flash file	`.swf`
vbe	Visual Basic™ encoded script file	`.vbe`
vbs	Visual Basic™ script file	`.vbs`
wsf	Microsoft™ Windows™ Script File	`.wsf`

xls	Microsoft™ Excel™ spreadsheet	`.xls`
		`.xla`
		`.xlt`
		`.xlm`

xlsx	Microsoft™ Office Excel™ (2007 or later) spreadsheet
	Microsoft™ Office Excel™ (2007 or later) macro-enabled spreadsheet
		`.xlsx`
		`.xlsb`
		`.xltx`
		`.xlsm`
		`.xlam`
		`.xltm`

xml	Microsoft™ Office 2003 XML file Microsoft™ Word™ 2003 XML document Microsoft™ Excel™ 2003 XML spreadsheet Microsoft™ PowerPoint™ 2003 XML presentation	`.xml`

Note

For the following script types, Virtual Analyzer does not perform analysis if file extension and file type do not match:

- bat
- cmd
- hta
- js
- jse
- ps1
- vbe
- vbs
- wsf

Submission Settings Tab Tasks

Procedure

1. To move file types to the **Analyzed** list:
   a. Select one or more file types in the **Not analyzed** list.
   b. Click **>>**.
   c. Click **Save**.
2. To move file types to the **Not analyzed** list:
   a. Select one or more file types in the **Analyzed** list.
   b. Click **<<**.
   c. Click **Save**.

3. To 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.

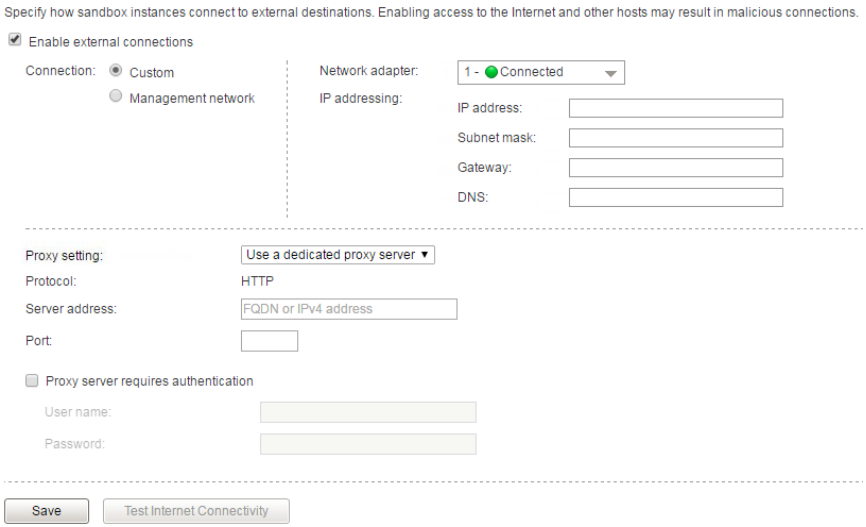
Procedure

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.

   - Management network: Default organization Intranet

     WARNING!

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

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

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

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

5. If the sandbox requires a proxy server for network connection, select **Use a dedicated proxy server**, and specify the following.
   - Server address
   - Port
   - User name: This option is only available if **Proxy server requires authentication** is enabled.
   - Password: This option is only available if **Proxy server requires authentication** is enabled.
6. Click **Save**.

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

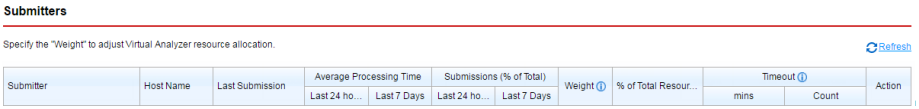
The cloud sandbox setting is automatically disabled if the TippingPoint Advanced Threat Protection Analyzer license expires.

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 4-17. 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.
% of Total Resources	Percentage of total Virtual Analyzer resources allocated to the Trend Micro product.
Timeout	Timeout period allotted for the Trend Micro product Specify a timeout period from 0 to 10000 minutes. A value of 0 means timeout is disabled. The number of samples affected by the timeout period for the past 24 hours is summarized in the **Count** column.
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. **Note** 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. • **Critical**: The event requires immediate attention • **Important**: The event requires observation • **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. • **Critical**: The event requires immediate attention • **Important**: The event requires observation • **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 6-30*.

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. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%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. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%ActiveApplianceName%` • `%ActiveApplianceIP%` • `%PassiveApplianceName%` • `%PasssiveApplianceIP%` • `%DateTime%` • `%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. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%LockedAccount%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%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. **Tip** 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 3-14*.
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. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%SandboxQueueThreshold%` • `%SandboxQueue%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%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. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%ComponentList%` • `%UpdateError%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%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. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%CPUThreshold%` • `%CPUUsage%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%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. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%MemThreshold%` • `%MemUsage%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%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. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%DiskThreshold%` • `%DiskUsage%` • `%FreeDiskSpace%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%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.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%ApplianceError%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%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.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%ActiveApplianceName%` • `%ActiveApplianceIP%` • `%PassiveApplianceName%` • `%PasssiveApplianceIP%` • `%DateTime%` • `%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. **Note** Specifying a low threshold may result in frequent generation of alerts, but each alert covers a unique set of detections.
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. **Note** Specifying a low threshold may result in frequent generation of alerts, but each alert covers a unique set of detections.

PARAMETER	DESCRIPTION
Subject	Specify the subject of the triggered alert notification.
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%HighRiskThreshold%` • `%TimeRange%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%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.

Parameter	Description
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%SyslogServer%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%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.
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%BackupServer%` • `%ApplianceName%` • `%ApplianceIP%` • `%DateTime%` • `%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.
Message	Specify the body of the triggered alert notification. Use the following tokens to customize your message: • `%ProductName%` • `%ProductShortName%` • `%ActiveApplianceName%` • `%ActiveApplianceIP%` • `%PassiveApplianceName%` • `%PasssiveApplianceIP%` • `%DateTime%` • `%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 High Availability Suspended Passive Primary Appliance Activated
`%ActiveApplianceName%`	The host name of the TippingPoint Advanced Threat Protection Analyzer active primary appliance	• ATP_Analyzer • ATP_Analyzer-ABC123	High Availability Restored High Availability Suspended Passive Primary Appliance Activated
`%ApplianceError%`	The error encountered by the appliance	• Not connected • Invalid API key • 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 • High Availability Restored • High Availability Suspended • Passive Primary Appliance Activated

Token	Description	Example	Where Allowed
`%ApplianceName%`	The host name of the TippingPoint Advanced Threat Protection Analyzer appliance	• ATP_Analyzer • ATP_Analyzer-ABC123	All • High Availability Restored • High Availability Suspended • Passive Primary Appliance Activated
`%BackupServer%`	The host name or IP address of the backup server	• my.example.com • 123.123.123.123 • 2001:0:3238:DFE1:63::FEFB	Backup Server Inaccessible
`%ComponentList%`	The list of components	• Advanced Threat Scan Engine • Deep Discovery Malware Pattern • IntelliTrap Exception Pattern • 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
`%PasssiveApplianceIP%`	The IPv4 address of the TippingPoint Advanced Threat Protection Analyzer passive primary appliance	123.123.123.123	High Availability Restored High Availability Suspended Passive Primary Appliance Activated
`%PassiveApplianceName%`	The host name of the TippingPoint Advanced Threat Protection Analyzer passive primary appliance	• ATP_Analyzer • ATP_Analyzer-ABC123	High Availability Restored High Availability Suspended 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 • 123.123.123.123 • 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 • 30 minutes • 1 hour • 12 hours • 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 • Unable to update: Deep Discovery Malware Pattern • 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** , 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

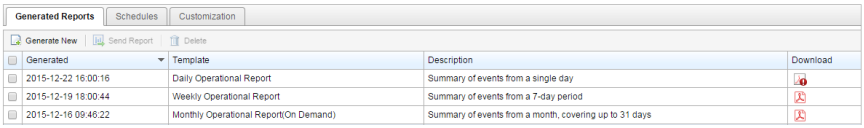
TASK	STEPS
Generate Reports	See *Generating Reports on page 5-26*.
Download Report	To download a report, go to the last column in the table and click the icon. Generated reports are available as PDF files.
Send Report	Select a report and then click **Send Report**. You can send only one report at a time.
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

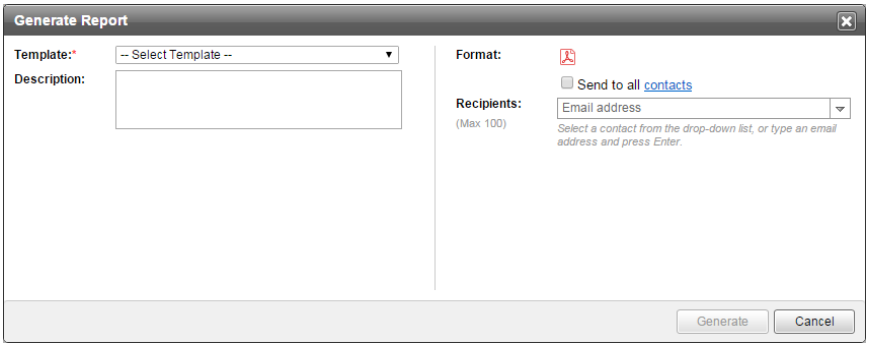
1. Go to **Alerts / Reports** > **Reports** > **Generated Reports**.

   The **Generated Reports** screen appears.



2. Click **Generate New**.

   The **Generate Report** window appears.



3. Configure report settings.

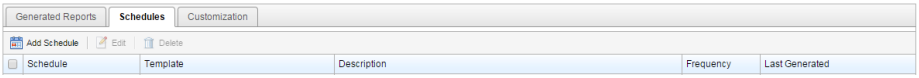
Option	Description
Template	Select an operational report template.
Description	Type a description that does not exceed 500 characters.
Range	Specify the covered date(s) based on the selected report template. • **Daily operational report**: Select any day prior to the current day. The report coverage is from 00:00:00 to 23:59:59 of each day. • **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. • **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. You can type a maximum of 100 email addresses, typing them one at a time. **Note** You must press ENTER after each email address. Do not type multiple email addresses separated by commas. Before specifying recipients, configure the SMTP settings in **Administration** > **System Settings** > **SMTP** . **Note** 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** , 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**.

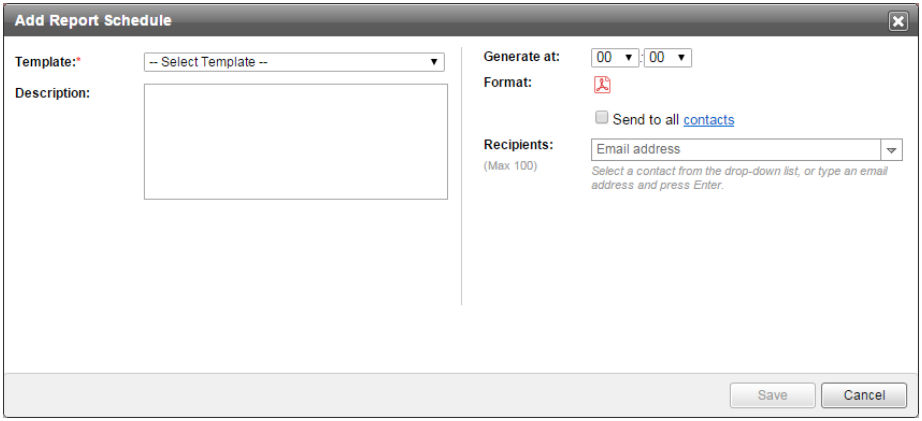
This tab includes the following options:

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*. 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:

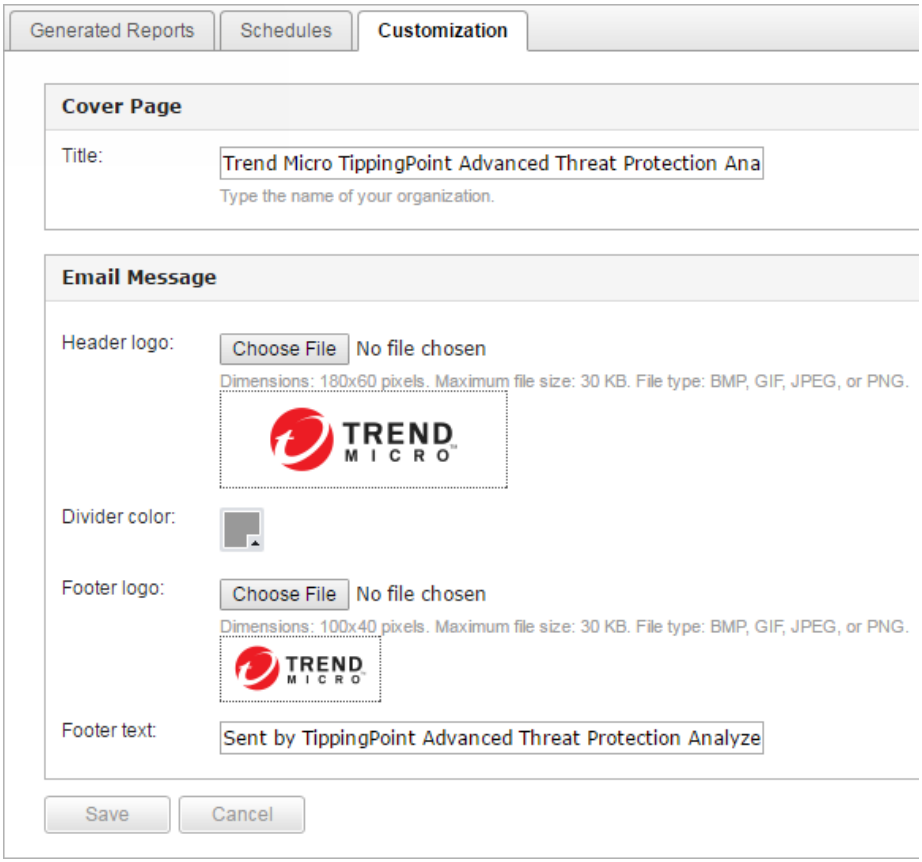
TABLE 5-23. Add Report Schedule Window Tasks

FIELD	STEPS
Template	Choose a template.
Description	Type a description.

FIELD	STEPS
Generate at	Configure the schedule according to the template you chose. 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. 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. 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. **Note** 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. 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**, 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. The following are the image requirements. • Dimensions: 180 x 60 pixels • Maximum file size: 30 KB • 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. 	Notification
Footer logo	Browse to the location of the logo. The following are the image requirements. • Dimensions: 100 x 40 pixels • Maximum file size: 30 KB • 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.

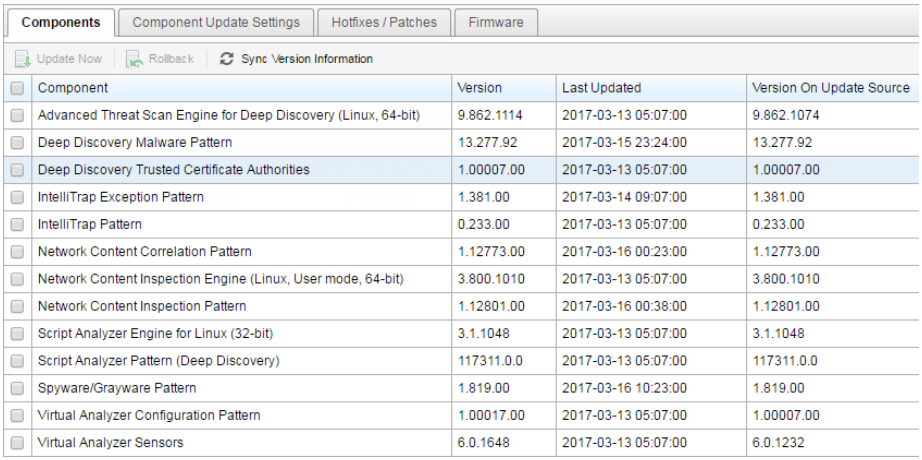
Updates

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 6-74*.

Components Tab

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



Component	Version	Last Updated	Version On Update Source
Advanced Threat Scan Engine for Deep Discovery (Linux, 64-bit)	9.862.1114	2017-03-13 05:07:00	9.862.1074
Deep Discovery Malware Pattern	13.277.92	2017-03-15 23:24:00	13.277.92
Deep Discovery Trusted Certificate Authorities	1.00007.00	2017-03-13 05:07:00	1.00007.00
IntelliTrap Exception Pattern	1.381.00	2017-03-14 09:07:00	1.381.00
IntelliTrap Pattern	0.233.00	2017-03-13 05:07:00	0.233.00
Network Content Correlation Pattern	1.12773.00	2017-03-16 00:23:00	1.12773.00
Network Content Inspection Engine (Linux, User mode, 64-bit)	3.800.1010	2017-03-13 05:07:00	3.800.1010
Network Content Inspection Pattern	1.12801.00	2017-03-16 00:38:00	1.12801.00
Script Analyzer Engine for Linux (32-bit)	3.1.1048	2017-03-13 05:07:00	3.1.1048
Script Analyzer Pattern (Deep Discovery)	117311.0.0	2017-03-13 05:07:00	117311.0.0
Spyware/Grayware Pattern	1.819.00	2017-03-16 10:23:00	1.819.00
Virtual Analyzer Configuration Pattern	1.00017.00	2017-03-13 05:07:00	1.00007.00
Virtual Analyzer Sensors	6.0.1648	2017-03-13 05:07:00	6.0.1232

TABLE 6-1. Components

COMPONENT	DESCRIPTION
Advanced Threat Scan Engine for Deep Discovery (Linux, 64-bit)	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.

Component	Description
Deep Discovery Malware Pattern	The Deep Discovery Malware Pattern contains information that helps TippingPoint 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.
Deep Discovery Trusted Certificate Authorities	Deep Discovery Trusted Certificate Authorities provides the trusted certificate authorities to verify PE signatures.
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.
Network Content Inspection Engine (Linux, User mode, 64-bit)	The Network Content Inspection Engine is used to perform network scanning.
Network Content Inspection Pattern	The Network Content Inspection Pattern is used by the Network Content Inspection Engine to perform network scanning.
Script Analyzer Engine for Linux (32-bit)	The Script Analyzer Engine analyzes web page scripts to identify malicious code.
Script Analyzer Pattern (Deep Discovery)	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.

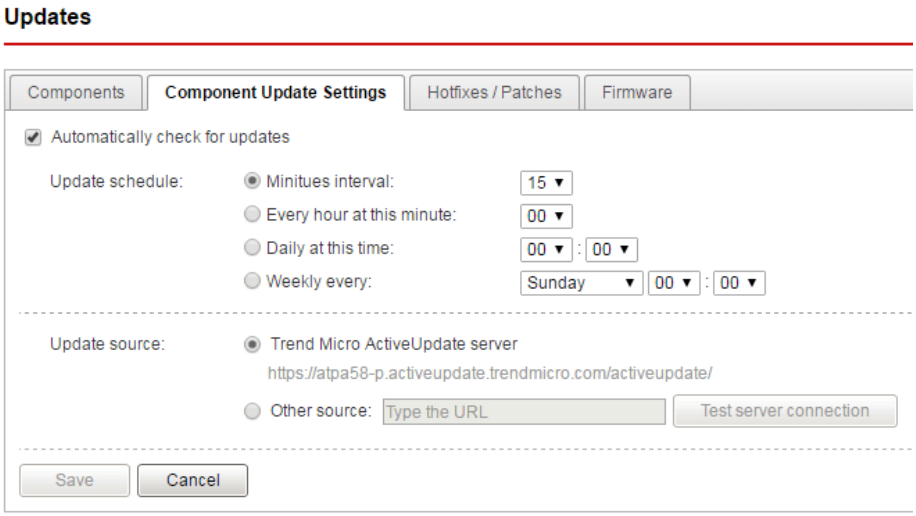
Component	Description
Virtual Analyzer Configuration Pattern	The Virtual Analyzer Configuration Pattern contains configuration information for Virtual Analyzer, such as supported threat types and supported file types.
Virtual Analyzer Sensors	The Virtual Analyzer Sensors are a collection of utilities used to execute and detect malware and to record behavior in Virtual Analyzer.

This screen includes the following options:

Option	Task
Update Now	Select one or more components, and click **Update Now** to manually update the selected components.
Rollback	Select one or more components, and click **Rollback** to revert the selected components to a previous version.
Sync Version Information	Click to retrieve the component version from the update source, and review if any of the components need updates. Update any component where the version displayed on the **Version on Update Source** column is greater than the current version. Additionally, TippingPoint Advanced Threat Protection Analyzer displays the version numbers of components with available updates in a red font.

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 set TippingPoint Advanced Threat Protection Analyzer to check for updates every 15 minutes. You may also specify the update to run at a specific time.

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. If you choose the ActiveUpdate server, verify that TippingPoint Advanced Threat Protection Analyzer has Internet connection. 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. **Note** When the IPv6 address is part of a URL, enclose the address in square brackets ([]). 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 6-28*.

Hotfixes / Patches Tab

Use the **Hotfixes / Patches** screen to apply hotfixes 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.

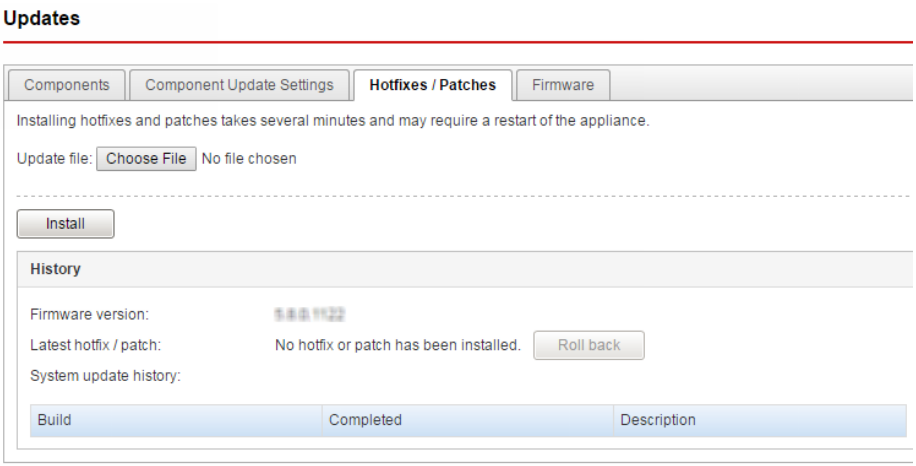


TABLE 6-2. Hotfixes / Patches

SYSTEM UPDATE	DESCRIPTION
Hotfix	A hotfix is a workaround or solution to a single customer-reported issue. Hotfixes are issue-specific, and are not released to all customers. **Note** A new hotfix may include previous hotfixes 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 hotfixes 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 hotfix and patch releases:

http://downloadcenter.trendmicro.com/

Installing a Hotfix / Patch

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

1. Detach the passive primary appliance.
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.

Procedure

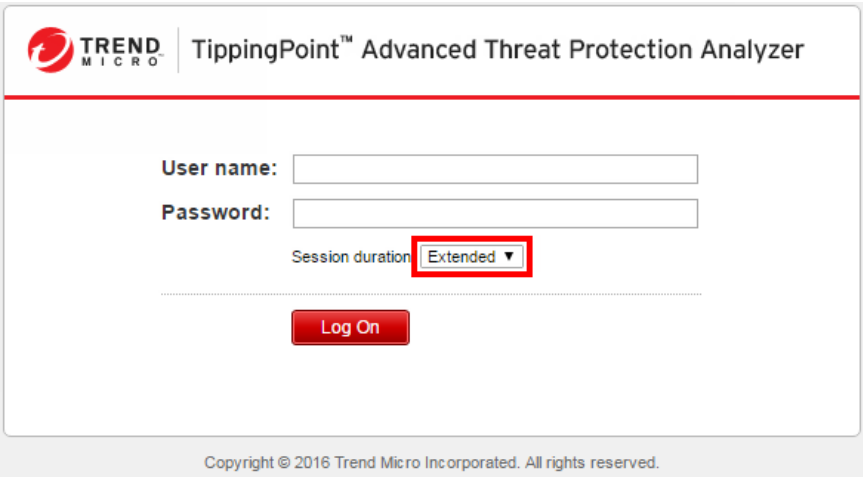
1. Obtain the product update file from Trend Micro.

- If the file is an official patch, download it from the download center.

  http://downloadcenter.trendmicro.com/

- If the file is a hotfix, 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** > **Hotfixes / 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** > **Hotfixes / Patches** screen.
8. Verify that the hotfix / patch displays in the **History** section as the latest update.

Rolling Back a Hotfix / Patch

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

1. Detach the passive primary appliance.
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.

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 hotfix / 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** > **Hotfixes / 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** > **Hotfixes / Patches** screen.
5. Verify that the hotfix / patch no longer displays in the **History** section.

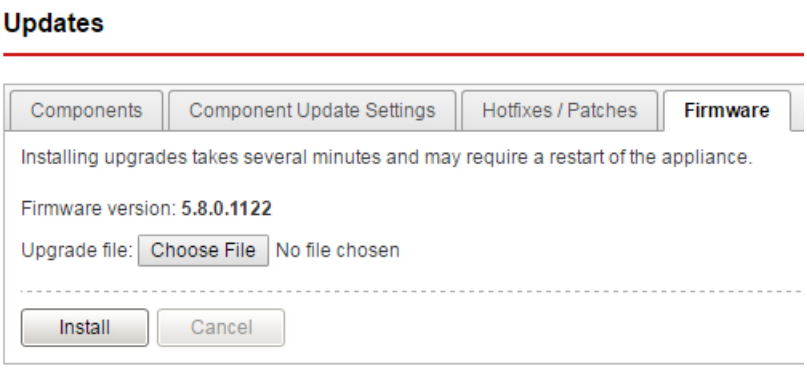
Firmware Tab

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.

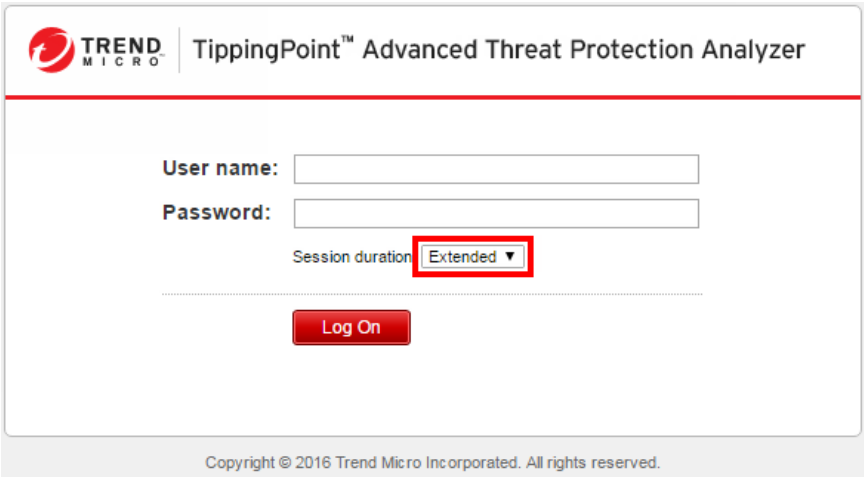
1. Detach the passive primary appliance.
2. On the active primary appliance, perform the tasks as described in the main task section below.
3. On the passive primary appliance, perform the tasks as described in the main task section below.
4. Add the passive primary appliance to the cluster again.

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.

Integrated Products/Services

The Integraded Products/Services screen, in **Administration** > **Integrated Products/Services**, includes the following tabs:

- *Log Settings Tab on page 6-13*
- *Smart Protection Tab on page 6-16*
- *Deep Discovery Director Tab on page 6-20*

Log Settings Tab

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

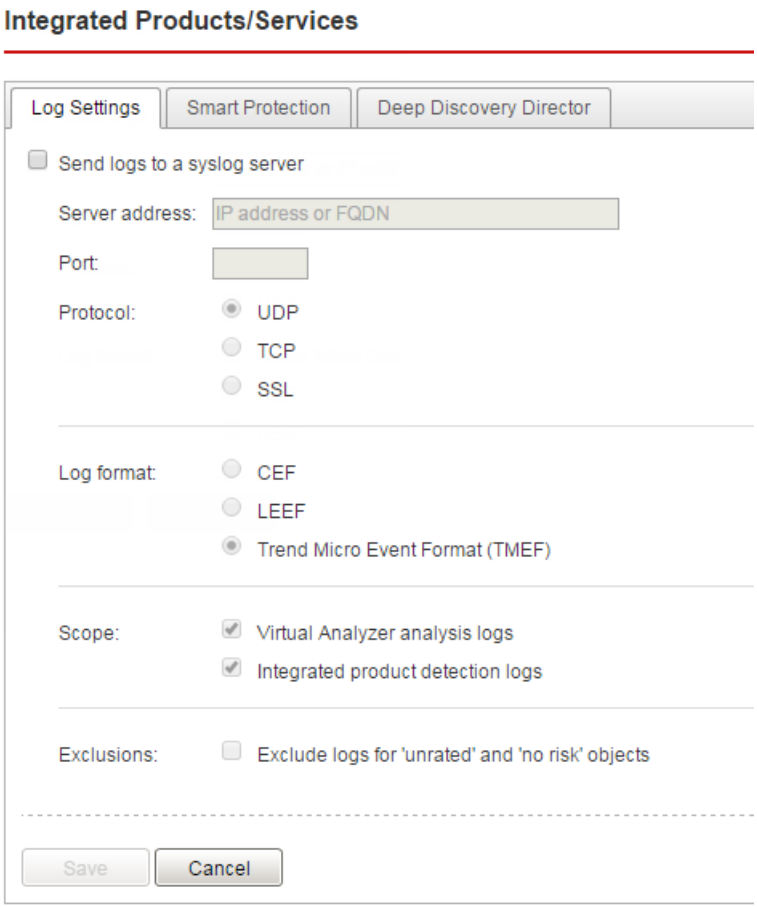
Configuring Syslog Settings

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** > **Integrated Products/Services** > **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:

- **UDP**: 514
- **TCP**: 601
- **SSL**: 443

5. Select the protocol to transport log content to the syslog server.
   - UDP
   - TCP
   - SSL
6. Select the format in which event logs are sent to the syslog server.
   - **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.
   - **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.
7. Select the scope of logs to send to the syslog server:
   - Virtual Analyzer analysis logs
   - Integrated product detection logs
8. (Optional) Select the logs to exclude from sending to the syslog server.
9. Click **Save**.

Smart Protection Tab

Trend Micro Smart Protection technology is a next-generation, in-the-cloud protection solution providing File and Web Reputation Services. By integrating Web Reputation Services, TippingPoint Advanced Threat Protection Analyzer can obtain reputation data for websites that users attempt to access. TippingPoint Advanced Threat Protection Analyzer logs URLs that Smart Protection technology verifies to be fraudulent or known sources of threats and then uploads the logs for report generation.

Note

TippingPoint Advanced Threat Protection Analyzer does not use the File Reputation Service that is part of Smart Protection technology.

TippingPoint Advanced Threat Protection Analyzer connects to a Smart Protection source to obtain web reputation data.

Reputation services are delivered through the Trend Micro Smart Protection Network and Smart Protection Server. These two sources provide the same reputation services and can be integrated individually or in combination. The following table provides a comparison.

TABLE 6-3. Smart Protection Sources

BASIS OF COMPARISON	TREND MICRO SMART PROTECTION NETWORK	SMART PROTECTION SERVER
Purpose	A globally scaled, Internet-based infrastructure that provides File and Web Reputation Services to Trend Micro products that integrate smart protection technology	Provides the same File and Web Reputation Services offered by Smart Protection Network but localizes these services to the corporate network to optimize efficiency
Administration	Hosted and maintained by Trend Micro	Installed and managed by Trend Micro product administrators
Connection protocol	HTTP	HTTP and HTTPS

Basis of Comparison	Trend Micro Smart Protection Network	Smart Protection Server
Usage	Use if you do not plan to install Smart Protection Server To configure Smart Protection Network as source, see *Configuring Smart Protection Settings on page 6-18*.	Use as primary source and the Smart Protection Network as an alternative source For guidelines on setting up Smart Protection Server and configuring it as source, see *Setting Up Smart Protection Server on page 6-18*.

About Smart Protection Server

Consideration	Description
Deployment	If you have previously installed a Smart Protection Server for use with another Trend Micro product, you can use the same server for TippingPoint Advanced Threat Protection Analyzer. While several Trend Micro products can send queries simultaneously, the Smart Protection Server may become overloaded as the volume of queries increases. Make sure that the Smart Protection Server can handle queries coming from different products. Contact your support provider for sizing guidelines and recommendations.
IP Address	Smart Protection Server and the VMware ESX/ESXi server (which hosts the Smart Protection Server) require unique IP addresses. Check the IP addresses of the VMware ESX/ESXi server and TippingPoint Advanced Threat Protection Analyzer to make sure that these IP addresses are not assigned to the Smart Protection Server.
Installation	For installation instructions and requirements, refer to the *Installation and Upgrade Guide* for Trend Micro Smart Protection Server at http://docs.trendmicro.com/en-us/enterprise/smart-protection-server.aspx.

Setting Up Smart Protection Server

Procedure

1. Install Smart Protection Server on a VMware ESX/ESXi server.
2. Configure Smart Protection Server settings from the TippingPoint Advanced Threat Protection Analyzer management console.

   For details, see *Configuring Smart Protection Settings on page 6-18*.

Note

- Smart Protection Server may not have reputation data for all URLs because it cannot replicate the entire Smart Protection Network database. When updated infrequently, Smart Protection Server may also return outdated reputation data.
- Enabling this option improves the accuracy and relevance of the reputation data.
- Disabling this option reduces the time and bandwidth to obtain the data.

Configuring Smart Protection Settings

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Smart Protection**.
2. Select **Enabled**.
3. Select a Smart Protection source:
   - Trend Micro Smart Protection Network™

     Trend Micro Smart Protection Network is a globally-scaled, cloud-based infrastructure providing reputation services to Trend Micro products that integrate Smart Protection technology. TippingPoint Advanced Threat Protection Analyzer connects to the Smart Protection Network using HTTP. Select this option if you do not plan to set up a Smart Protection Server.

- Smart Protection Server

  Smart Protection Server does the following:

  - Provides Web Reputation Services as offered by Smart Protection Network
  - Relays these services to the global Trend Micro Smart Protection Network for network efficiency

  As a Trend Micro product administrator, you must set up and maintain this server. Select this option if you have already set up a server.

4. To select Smart Protection Server, you must configure it.

   a. Specify the Smart Protection Server IP address or fully qualified domain name and port number.

      Obtain the IP address by going to **Smart Protection** > **Reputation Services** > **Web Reputation** on the Smart Protection Server console.

      The IP address forms part of the URL listed on the screen.

   b. (Optional) Select **Connect using a proxy server** if proxy settings for TippingPoint Advanced Threat Protection Analyzer have been configured for use with Smart Protection Server connections.

      Note

      If proxy settings are disabled, Smart Protection Server will connect to TippingPoint Advanced Threat Protection Analyzer directly.

5. (Optional) Select **Connect to global services using Smart Protection Server** to configure TippingPoint ATP Analyzer to query global Smart Protection services.

   - (Optional) If your organization uses a CA certificate, select **Use certificate** and click **Choose File** or **Browse** to locate the certificate file.

     - (Optional) If your organization uses a Certificate Revocation List, select **Use CRL** and click **Choose File** or **Browse** to locate the Certificate Revocation List file.

Important

TippingPoint ATP Analyzer supports connection to global services only if Smart Protection Server version 3.0 Patch 2 is used.

Note

When **Smart Protection Server** is selected as Smart Protection source, but the **Connect to global services using Smart Protection Server** option is disabled, the following services and the ability to test their connectivity will be disabled:

- Certified Safe Software Service (CSSS)
- Community File Reputation
- Web Inspection Service
- Smart Feedback

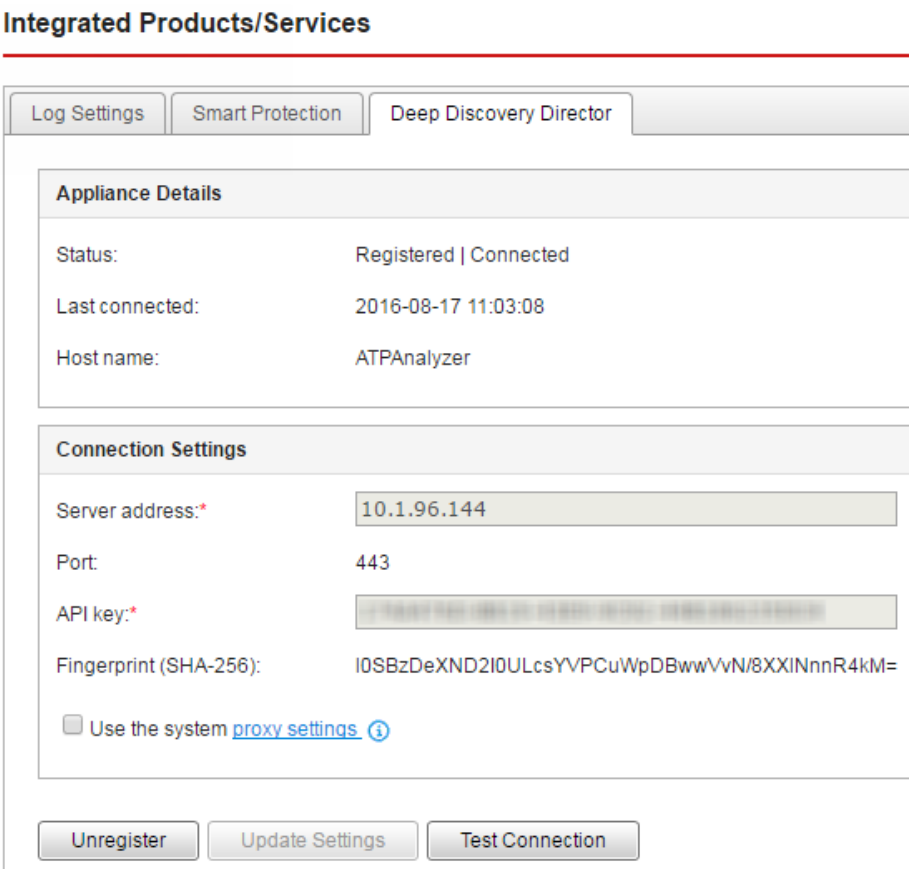
6. Click **Save**.

Deep Discovery Director Tab

Trend Micro Deep Discovery Director 1.1 is an on-premises management solution that enables centralized deployment of product updates, product upgrades, and Virtual Analyzer images to TippingPoint products, as well as configuration replication of TippingPoint products. To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options such as distributed mode and consolidated mode.

Important

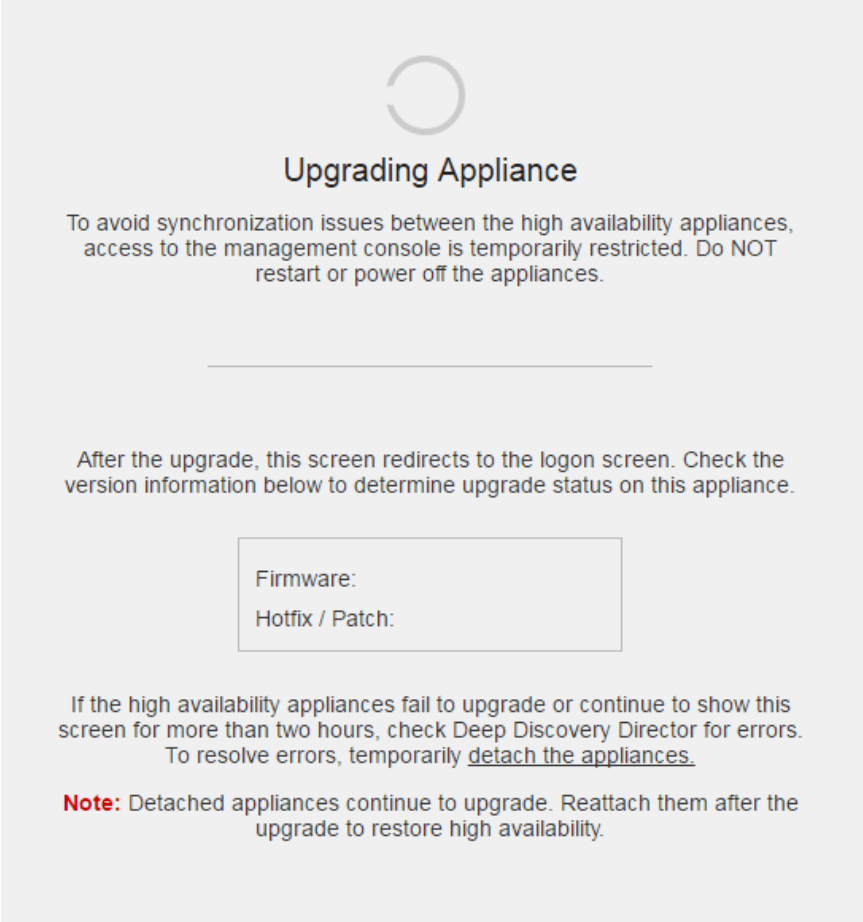
TippingPoint Advanced Threat Protection Analyzer does not support integration with Deep Discovery Director.



Deploying updates or upgrades to TippingPoint Advanced Threat Protection Analyzer appliances that are configured in a high availability cluster will temporarily:

- Detach the high availability appliances and suspend high availability

- Restrict access to the management console and display a static information screen



After the update or upgrade completes, the detached appliances will automatically reattach and restore high availability.

Important

- Before deploying updates or upgrades, ensure that the appliances are not executing any task.
- Avoid detaching appliances while an upgrade is in progress.
- If the appliances fail to upgrade or continue to show the **Upgrading Appliance** screen for more than two hours, check Deep Discovery Director for errors. To resolve errors, temporarily detach the appliances. Detached appliances continue to upgrade. After the upgrade, manually attach the appliances again to restore high availability.

The Deep Discovery Director screen displays the following information:

TABLE 6-4. Deep Discovery Director Fields

FIELD	INFORMATION
Status	The following appliance statuses can be displayed: • Not registered: The appliance is not registered to Deep Discovery Director. • Registered | Connected: The appliance is registered and connected to Deep Discovery Director. • Registered | Unable to connect: The appliance is registered to Deep Discovery Director, but unable to connect. Verify that the Deep Discovery Director network settings are valid. • Registered | Untrusted fingerprint: The appliance is registered to Deep Discovery Director, but the connection was interrupted. To restore the connection, trust the new fingerprint.
Last connected	The last time this appliance connected to Deep Discovery Director.
Host name	The host name of this appliance.
Server address	The Deep Discovery Director server address.
Port	The Deep Discovery Director port.
API key	The Deep Discovery Director API key.

FIELD	INFORMATION
Fingerprint (SHA-256)	The Deep Discovery Director fingerprint.
Use the system proxy settings	Select to use the system proxy settings to connect to Deep Discovery Director.

Note

The Deep Discovery Director management console is used to deploy or replicate a Virtual Analyzer image or configuration to a primary appliance. This is not required for secondary appliances since they are set to automatically sync Virtual Analyzer images or configuration from the primary appliance.

Registering to Deep Discovery Director

The following procedure is for registering to Deep Discovery Director. If you have already registered and want to change the connection settings, you must first unregister.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director**
2. Under **Connection Settings**, type the **Server address** for Deep Discovery Director.
3. Under **Connection Settings**, type the **API key** for Deep Discovery Director.

   Note

   You can find this information on the **Help** screen on the management console of Deep Discovery Director.

4. (Optional) If you have configured proxy settings for TippingPoint Advanced Threat Protection Analyzer and want to use these settings for Deep Discovery Director connections, select **Use the system proxy settings**.

Note

This setting can be changed after registering to Deep Discovery Director.

To update this setting without unregistering from Deep Discovery Director, click **Update Settings**.

5. Click **Register**.

   The **Status** changes to **Registered** and **Connected**.

Note

- If the Deep Discovery Director fingerprint changes, the connection is interrupted and the **Trust** button appears. To restore the connection, verify that the Deep Discovery Director fingerprint is valid and then click **Trust**.
- After the registration process is complete, the **Test Connection** button appears. You can click **Test Connection** to test the connection to Deep Discovery Director.
- If you are using TippingPoint Advanced Threat Protection Analyzer in a load-balancing cluster, registering the primary appliance will automatically register all secondary appliances.

Unregistering from Deep Discovery Director

Follow this procedure to unregister from Deep Discovery Director or before registering to another Deep Discovery Director.

Procedure

1. Go to **Administration** > **Integrated Products/Services** > **Deep Discovery Director**
2. Click **Unregister**.

   The **Status** changes to **Not registered**.

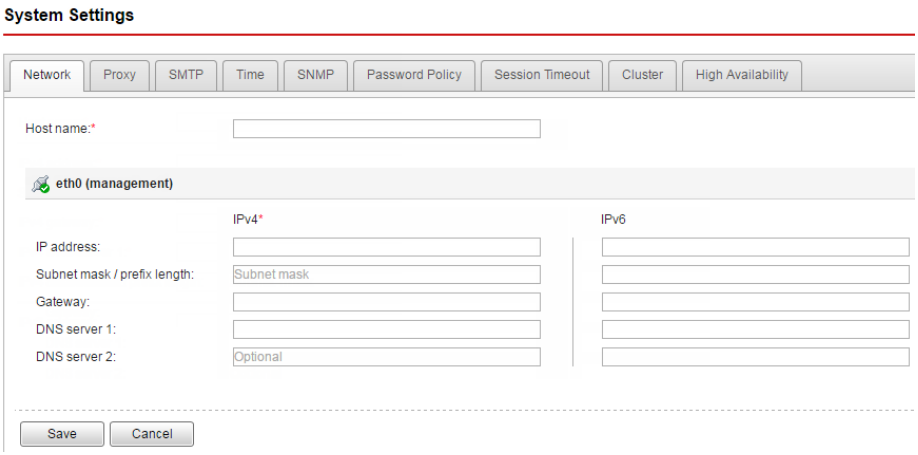
System Settings

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

- *Network Tab on page 6-27*
- *Proxy Tab on page 6-28*
- *SMTP Tab on page 6-30*
- *Time Tab on page 6-31*
- *SNMP Tab on page 6-34*
- *Password Policy Tab on page 6-40*
- *Session Timeout Tab on page 6-41*
- *Cluster Tab on page 6-41*
- *High Availability Tab on page 6-56*

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.

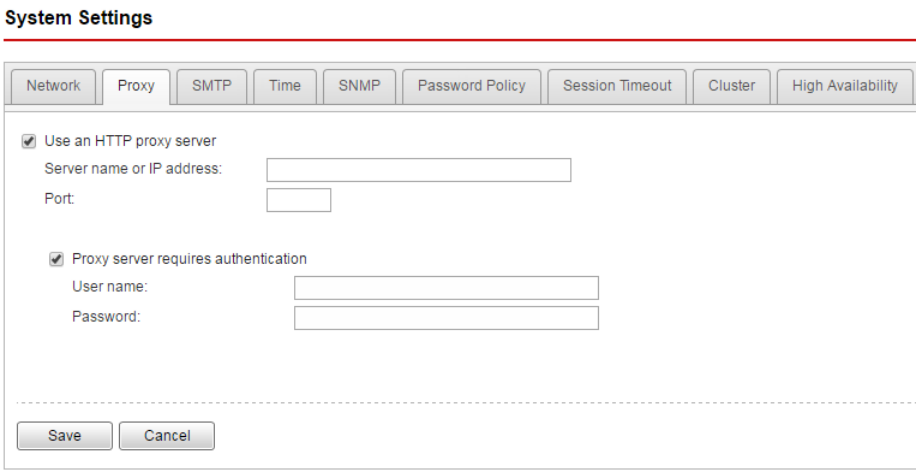
The following table lists configuration limitations.

TABLE 6-5. Configuration Limitations

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

Proxy Tab

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



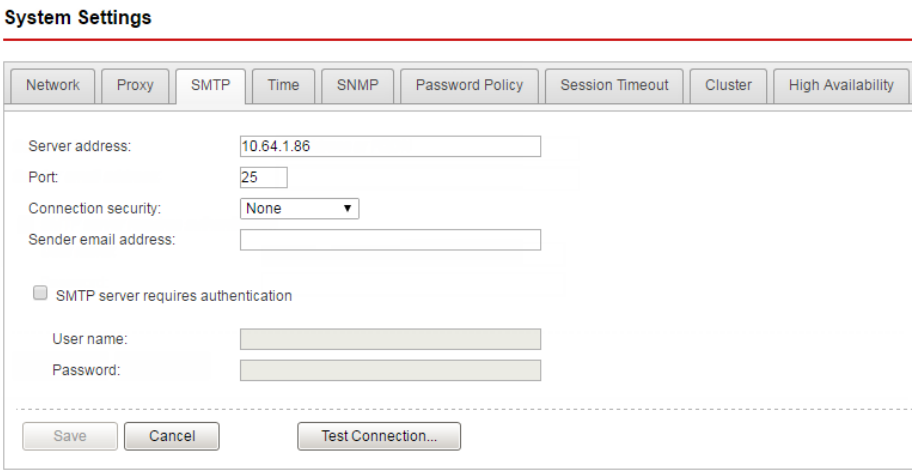
Configure the following settings.

TABLE 6-6. Proxy Tab Tasks

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

SMTP Tab

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



Procedure

1. Go to **Administration** > **System Settings** and click the **SMTP** tab.
2. Specify the following details:

TABLE 6-7. SMTP Tab Tasks

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

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

3. (Optional) To test the connection to the external SMTP server, do the following:
   a. Click **Test Connection**.
   b. Type the recipient email address.
   c. Click **OK**.

   Note
   TippingPoint Advanced Threat Protection Analyzer does not send a test email message to the recipient.

4. Click **Save**.

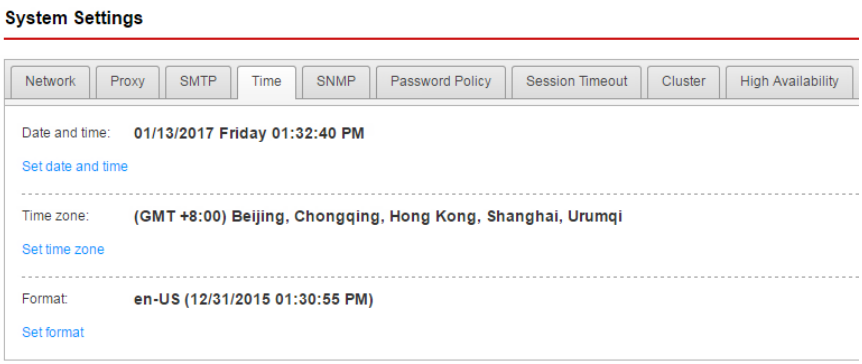
Time Tab

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.

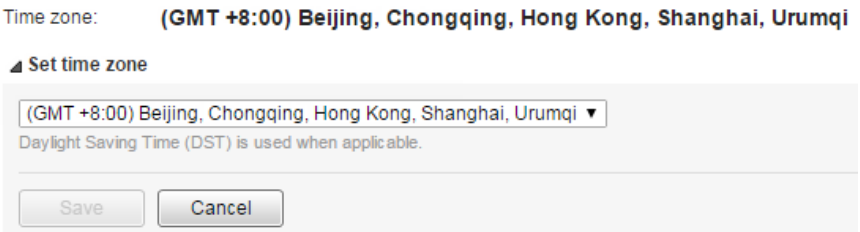
3. Select one of the following methods and configure the applicable settings.

   - 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.

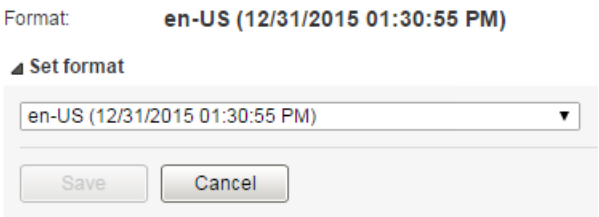
Note

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.

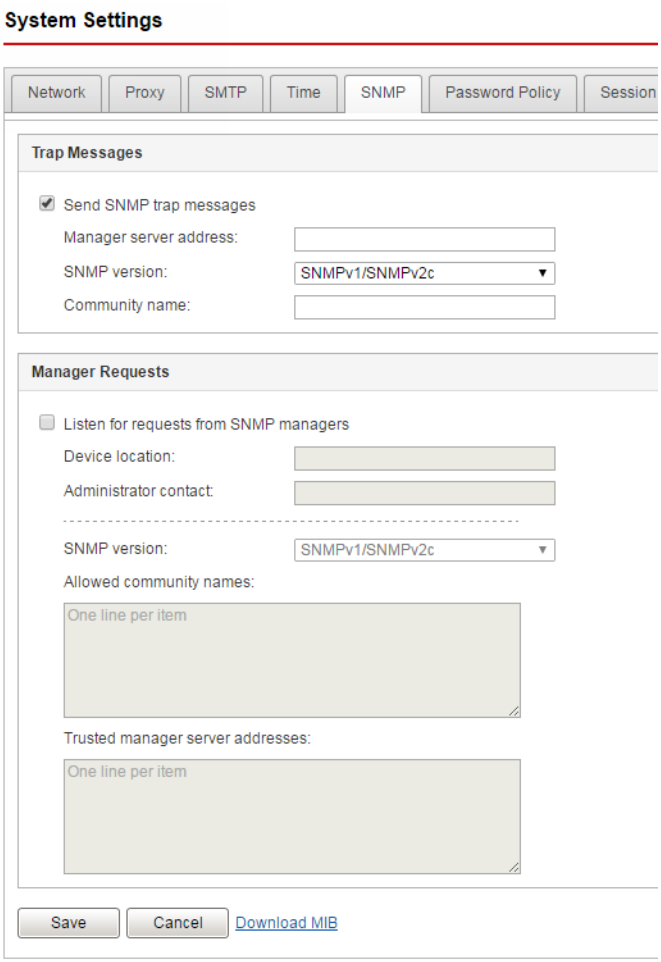
10. Click **Save**.

SNMP Tab

Simple Network Management Protocol (SNMP) is a protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.

A Simple Network Management Protocol (SNMP) trap is a method of sending notifications to network administrators who use management consoles that support this protocol.

On TippingPoint Advanced Threat Protection Analyzer, use the **Administration** > **System Settings** > **SNMP** tab to perform the following tasks:



- Configure the appliance to send trap messages

  For details, see *Configuring Trap Messages on page 6-36*.

- Configure the appliance to listen for manager requests

  For details, see *Configuring Manager Requests on page 6-37*.

Configuring Trap Messages

A SNMP Trap Message is the notification message sent to the SNMP server when events that require administrative attention occur.

Procedure

1. Go to **Administration** > **System Settings** > **SNMP**.
2. Under **Trap Messages**, select **Send SNMP trap messages**.
3. Specify the trap message settings.

OPTION	DESCRIPTION
Manager Server address	Specify the manager server address.
SNMP version	Select the SNMP version: • SNMPv1/SNMPv2c • SNMPv3 If you use SNMPv3, configure the SNMP server as follows: • Context Name: `""` (default context) • Context Engine ID: `<Auto>` • (Optional) MD5 Authentication protocol: `HMAC-MD5` • (Optional) DES Privacy protocol: `CBC-DES`
Community name	Specify a community name.

Option	Description
Security model	Select the security model: • No authentication or privacy • Authenticated • Authenticated with privacy
User name	Specify the user name.
Password	Specify the password.
Privacy passphrase	Specify the privacy passphrase.

Note

Before configuring the appliance, set up the SNMP server first using the same SNMP version, community name, security model, user name, password, and privacy passphrase.

4. Click **Save**.

5. (Optional) Click **Download MIB** to download the Management Information Database (MIB) files.

   - Users can open the MIB files to view all network objects that can be monitored and managed using the SNMP protocol, or import them into management consoles that support this protocol.

   - For a list of TippingPoint Advanced Threat Protection Analyzer supported SNMP object identifiers (OID), see *SNMP Object Identifiers on page B-1*.

Configuring Manager Requests

SNMP managers can use SNMP protocol commands to request TippingPoint Advanced Threat Protection Analyzer system information.

Procedure

1. Go to **Administration** > **System Settings** > **SNMP**.
2. Under **Manager requests**, select **Listen for requests from SNMP managers**.
3. Specify the manager request settings.

OPTION	DESCRIPTION
Device location	Specify the location of this appliance.
Administrator contact	Specify the administrator contact of this appliance.
SNMP version	Select the SNMP version: • SNMPv1/SNMPv2c • SNMPv3 If you use SNMPv3, configure the SNMP server as follows: • Context Name: `""` (default context) • Context Engine ID: `<Auto>` • (Optional) MD5 Authentication protocol: `HMAC-MD5` • (Optional) DES Privacy protocol: `CBC-DES`
Allowed community names	Specify a maximum of 5 community names.
Security model	Select the security model: • No authentication or privacy • Authenticated • Authenticated with privacy
User name	Specify the user name.
Password	Specify the password.

Option	Description
Privacy passphrase	Specify the privacy passphrase.
Trusted manager server addresses	Specify a maximum of 5 trusted manager server addresses.

Note

Before configuring the appliance, set up the SNMP server first using the same SNMP version, community name, security model, user name, password, and privacy passphrase.

4. Click **Save**.

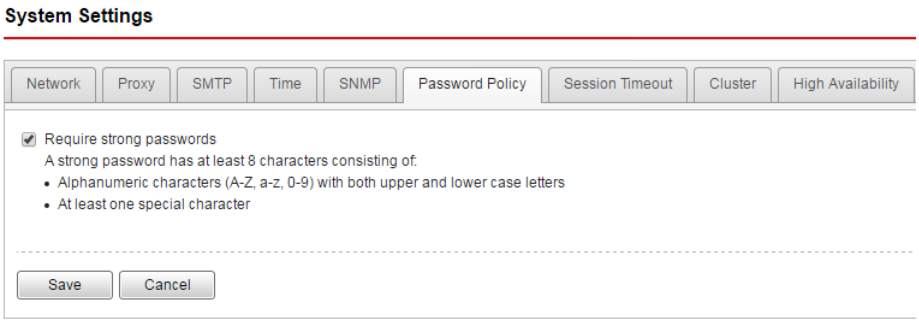
5. (Optional) Click **Download MIB** to download the Management Information Database (MIB) files.

   - Users can open the MIB files to view all network objects that can be monitored and managed using the SNMP protocol, or import them into management consoles that support this protocol.

   - For a list of TippingPoint Advanced Threat Protection Analyzer supported SNMP object identifiers (OID), see *SNMP Object Identifiers on page B-1*.

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.

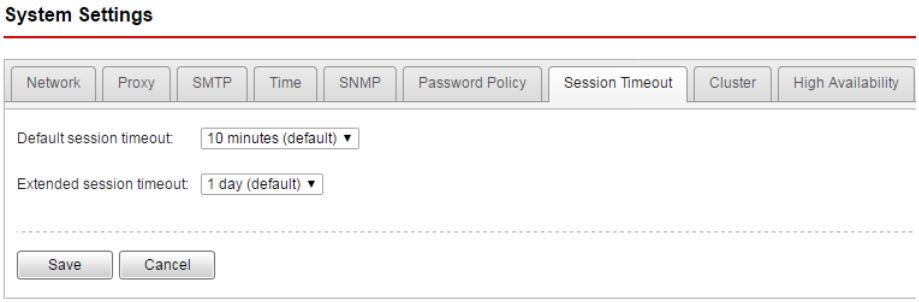


When strong passwords are required, a user submits a new password, and the password policy determines whether the password meets your company's established requirements.

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 logon 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.

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 6-8. 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 6-9. Cluster Configuration Modes

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

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

Configuration Mode	Description

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

Nodes List

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

The Nodes list contains the following information:

TABLE 6-10. Nodes List Columns

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

Column	Description

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

COLUMN	DESCRIPTION

Action	Actions that can be executed depending on the appliance mode and status.
	• For active primary appliance:
	  • **Swap**: Swap the roles of the primary appliances. Sets the current passive primary appliance to primary mode (active) and the current active primary appliance to primary mode (passive). Appears when the passive primary appliance has synced all settings from the active primary appliance. For details, see *Swapping the Active Primary Appliance and the Passive Primary Appliance on page 6-50*
	• For passive primary appliance:
	  • **Detach**: Detach the passive primary appliance. Disables high availability and allows the passive primary appliance to be used as a standalone appliance. Appears when the passive primary appliance has synced all settings from the active primary appliance. For details, see *Detaching the Passive Primary Appliance from the Cluster on page 6-50*
	  • **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 6-50*
	• For secondary appliances:
	  • **Remove**: Remove inaccessible secondary appliance. Affects object processing capacity. Secondary appliances attempt to connect to the active primary appliance every 10 seconds. Appears when the active primary appliance does not receive a heartbeat from the secondary appliance within one minute. For details, see *Removing a Secondary Appliance from the Cluster on page 6-53*

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 6-11. High Availability Clustering Requirements

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

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

Note

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

Procedure

1. Perform the installation and deployment tasks as described in 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 Settings** and click the **Cluster** tab.

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

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

   d. Click **Test Connection**.

   e. Click **Save**.

   You will be redirected to the appliance standby screen.

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

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

  Important

  While the appliance is syncing, it cannot:

  - Take over as active primary appliance
  - Switch to another mode

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

Swapping the Active Primary Appliance and the Passive Primary Appliance

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

Procedure

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

Detaching the Passive Primary Appliance from the Cluster

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

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

Important

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

Procedure

1. On the management console of the active primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.
2. Click **Detach** to detach the passive primary appliance from the cluster.

Removing the Passive Primary Appliance from the Cluster

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

Procedure

1. On the management console of the active primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.
2. Wait for **Remove** to appear next to the passive primary appliance in the nodes list.
3. Click **Remove** to remove the passive primary appliance from the cluster.

Note

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

Adding a Secondary Appliance to the Cluster

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

To view the appliance firmware, hotfix, and patch version, see *About Screen on page 6-77*.

Update or upgrade the appliance firmware, hotfix, and patch version 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.
- When using high availability, use the virtual IP address to register.

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 Settings** and click the **Cluster** tab.

b. Select **Secondary mode**.

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

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

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

e. Click **Test Connection**.

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

f. Click **Save**.

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

a. Configure the sandbox network connection setting.

For details, see *Enabling External Connections on page 4-50*.

> **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 4-53*.

c. Configure the appliance network settings.

For details, see *Network Tab on page 6-27*.

d. Add accounts.

For details, see *Accounts Tab on page 6-57*.

Removing a Secondary Appliance from the Cluster

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

Procedure

1. On the management console of the active primary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.
2. Wait for **Remove** to appear next to the secondary appliance in the nodes list.

   Note

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

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

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

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

Replacing the Active Primary Appliance with a Secondary Appliance

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

Tip

Trend Micro recommends deployment of a passive primary appliance for high availability. For details, see *Adding a Passive Primary Appliance to the Cluster on page 6-48*.

Important

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

Procedure

1. Power off the active primary appliance.
2. Select a secondary appliance from the same cluster and configure it as the new active primary appliance.
   a. On the management console of the secondary appliance, go to **Administration** > **System Settings** and click the **Cluster** tab.
   b. Select **Primary mode (active)**.
   c. Click **Save**.
3. Configure the IP address of the new active primary appliance.

   For details, see *Network Tab on page 6-27*.

   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.

Moving High Availability Cluster Appliances

Important

If you need to move high availability cluster appliances to another location, the passive node must always be powered off first and powered on last.

Procedure

1. Power off the passive primary appliance.
2. Power off the active primary appliance on the **Administration** > **System Maintenance** > **Power Off/Restart** tab.
3. Move both appliances to the new location.
4. Connect each appliance to the management network using eth0.
5. Connect both appliances directly to each other using eth3.
6. Power on the active primary appliance.
7. Power on the passive primary appliance.

Changing the IP Segment of High Availability Clusters

The management console supports changing the virtual IP address and management IP address only if they are in the same network segment. However, if you need to move the IP address to another network segment, nodes must be detached, re-configured and then set up again.

Procedure

1. Detach the passive primary appliance.
2. On active primary appliance UI, delete the virtual IP address, and then configure the management IP address and virtual IP address to match the IP address in the new network segment.

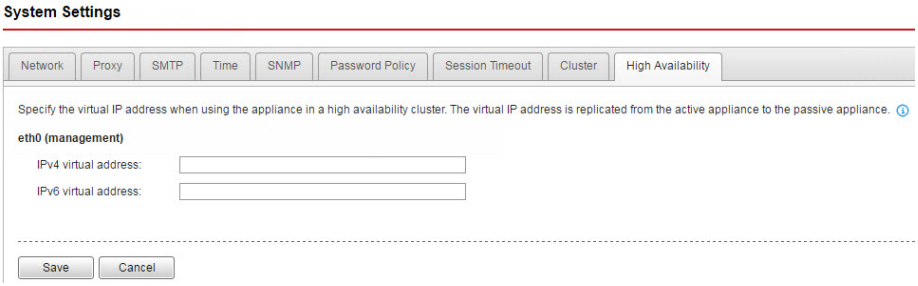
3. On passive primary appliance UI, configure the management IP address to match the IP address in the new network segment

4. Add the passive primary appliance to the cluster again.

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.

TABLE 6-12. Configuration Limitations when Using High Availability

FIELD	LIMITATION
IPv4 virtual address	• Cannot be used by another host • Must differ from IPv4 address • Must be in the same network segment as IPv4 address

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

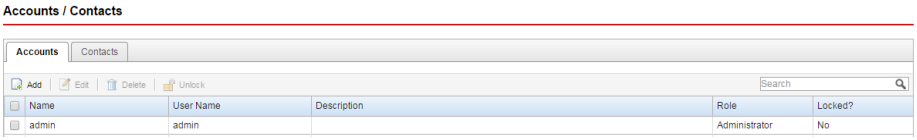
Accounts / Contacts

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

- *Accounts Tab on page 6-57*
- *Contacts Tab on page 6-61*

Accounts Tab

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



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

This screen includes the following options.

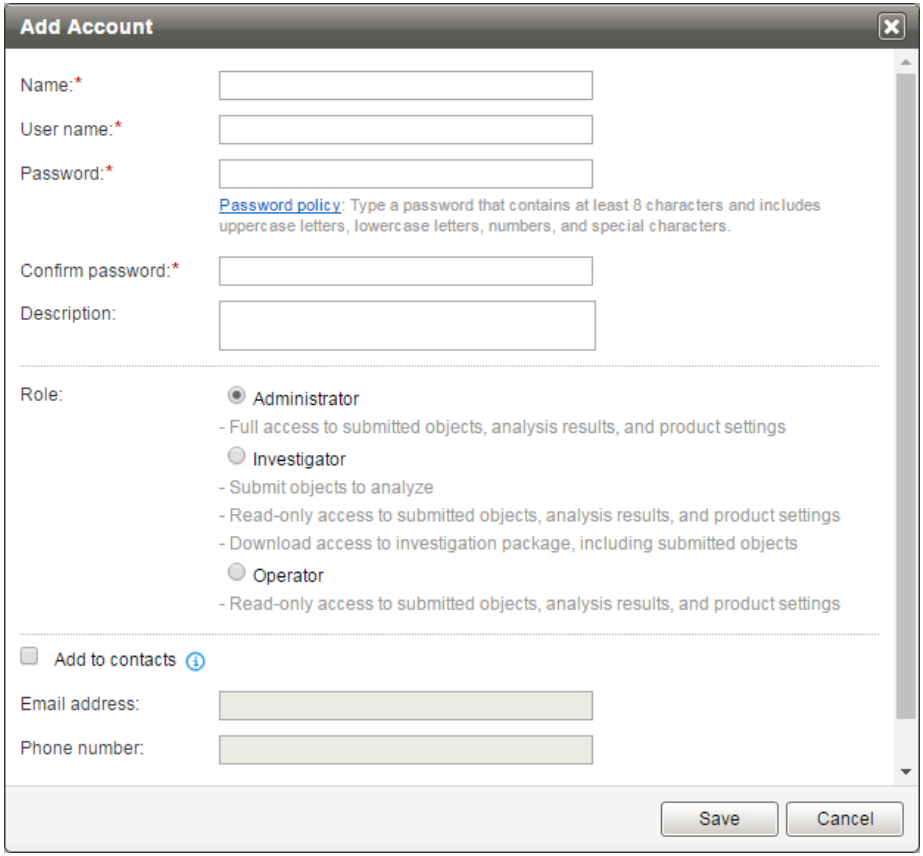
TABLE 6-13. Accounts Tasks

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 6-59*.
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 6-59*. Only one user account can be edited at a time.
Delete	Select one or more user accounts to delete and then click **Delete**. **Important** • You cannot delete the default TippingPoint Advanced Threat Protection Analyzer administrator account. • You cannot delete the logged-on account.
Unlock	TippingPoint Advanced Threat Protection Analyzer includes a security feature that locks an account in case the user typed an incorrect password five times in a row. This feature cannot be disabled. Accounts locked this way, including administrator accounts, unlock automatically after ten minutes. The administrator can manually unlock accounts that have been locked. Only one user account can be unlocked at a time.
Sort Column Data	Click a column title to sort the data below it.
Search	If there are many entries in the table, type some characters in the Search text box to narrow down the entries. As you type, the entries that match the characters you typed are displayed. TippingPoint Advanced Threat Protection Analyzer searches all cells in the table for matches.

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

Add Account Window

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



This window includes the following options.

TABLE 6-14. Add Account Window

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

Contacts Tab

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

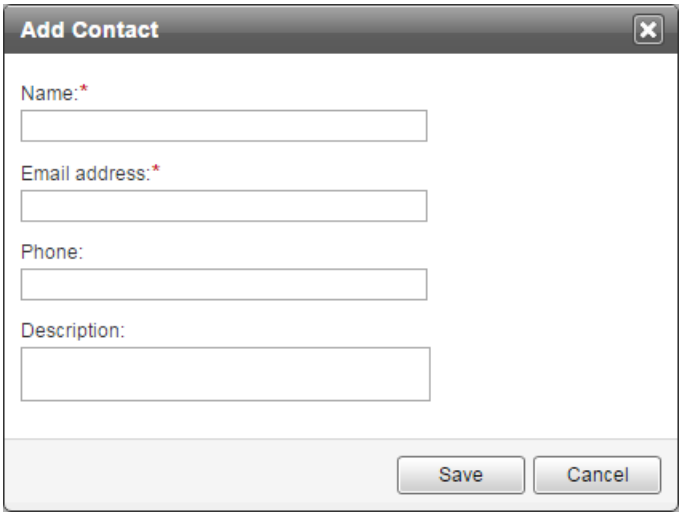
This screen includes the following options.

TABLE 6-15. 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 6-61*.
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 6-61*. Only one contact can be edited at a time.
Delete	Select one or more contacts to delete and then click **Delete**.
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 click **Add Contact** on the **Contacts** tab.



This window includes the following options.

TABLE 6-16. 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.

System Logs

TippingPoint Advanced Threat Protection Analyzer maintains system 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 system logs in the appliance hard drive.

Querying System Logs

Procedure

1. Go to **Administration** > **System 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 system logs whose user names contain the keyword.
5. Click **Export All** to export the system log to a `.csv` file.

System Maintenance

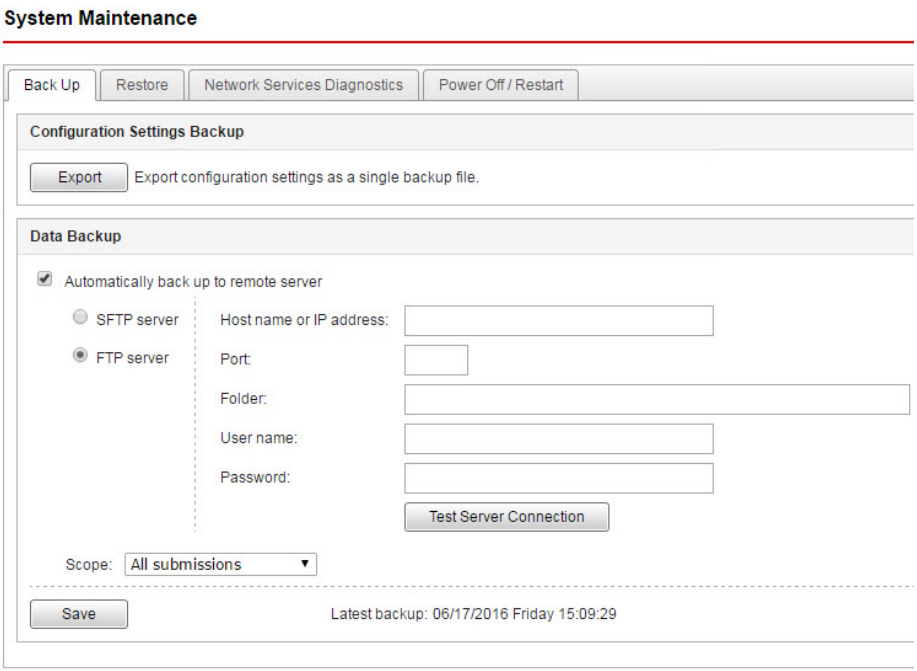
The **System Maintenance** screen, in **Administration** > **System Maintenance**, includes the following tabs:

- *Back Up Tab on page 6-64*
- *Restore Tab on page 6-67*
- *Network Services Diagnostics Tab on page 6-68*
- *Power Off / Restart Tab on page 6-69*

Back Up Tab

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

- *Configuration Settings Backup on page 6-64*
- *Data Backup on page 6-66*



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 6-17. Backed Up Configuration Settings

SCREEN	TAB
Dashboard	Not applicable (all widgets and settings)
Virtual Analyzer > **Exceptions**	Not applicable
Virtual Analyzer > **Suspicious Objects**	User-defined Match List
Virtual Analyzer > **Sandbox Management**	Archive Passwords
	Submission Settings
	Smart Feedback
	Cloud Sandbox
Alerts / Reports > **Alerts**	Rules
Alerts / Reports > **Report**	Schedules
	Customization
Administration > **Updates**	Component Update Settings
Administration > **Integrated Products/ Services**	Log Settings Smart Protection
Administration > **System Settings**	Proxy
	SMTP
	Time (time zone and format)
	SNMP
	Password Policy
	Session Timeout
Administration > **Accounts / Contacts**	Accounts
	Contacts
Administration > **System Maintenance**	Data back up

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 4-22*.

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 or 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

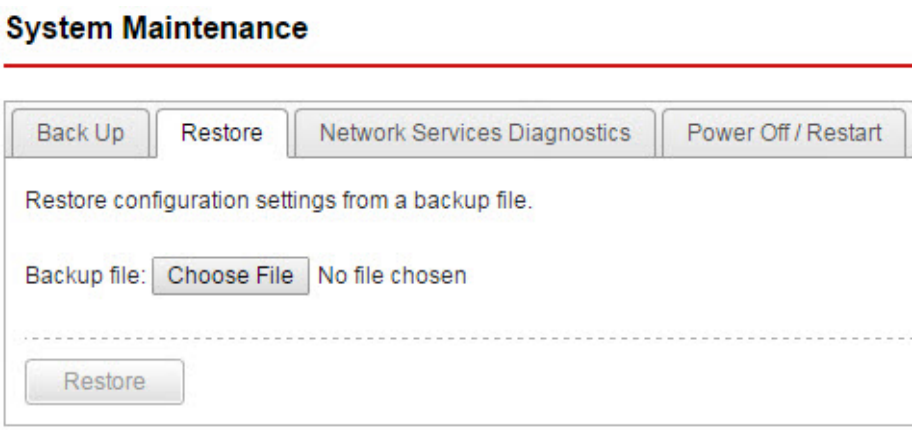
The **Restore** tab restores configuration settings from a backup file.

Note

For information on creating a backup file of the configuration settings, see *Back Up Tab on page 6-64*.

Important

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



Procedure

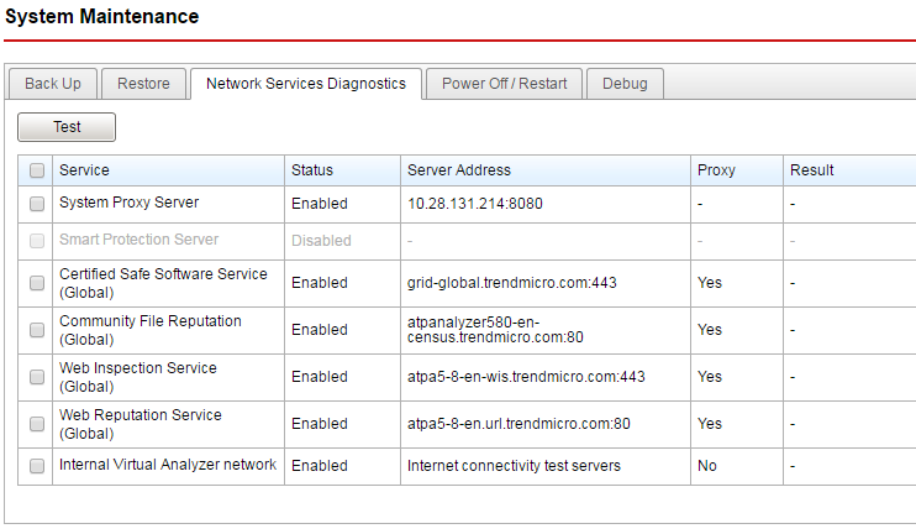
1. Click **Choose File** or **Browse**.

2. Select the backup file.

3. Click **Restore**.

Network Services Diagnostics Tab

You can use the **Network Services Diagnostics** screen to test the network connections for the internal Virtual Analyzer and other network services.



Service	Status	Server Address	Proxy	Result
System Proxy Server	Enabled	10.28.131.214:8080	-	-
Smart Protection Server	Disabled	-	-	-
Certified Safe Software Service (Global)	Enabled	grid-global.trendmicro.com:443	Yes	-
Community File Reputation (Global)	Enabled	atpanalyzer580-en-census.trendmicro.com:80	Yes	-
Web Inspection Service (Global)	Enabled	atpa5-8-en-wis.trendmicro.com:443	Yes	-
Web Reputation Service (Global)	Enabled	atpa5-8-en.url.trendmicro.com:80	Yes	-
Internal Virtual Analyzer network	Enabled	Internet connectivity test servers	No	-

Procedure

1. Select one or more enabled services and click **Test**.

   Wait for the connection test to complete. The time required depends on the network environment and the number of services selected. View the connection test result in the **Result** column.

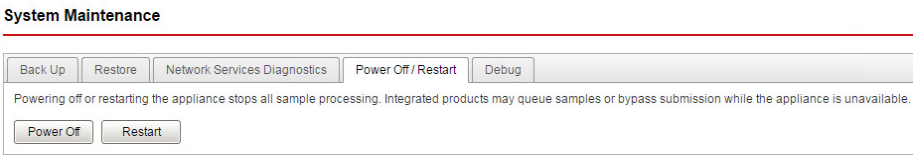
Power Off / Restart Tab

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.

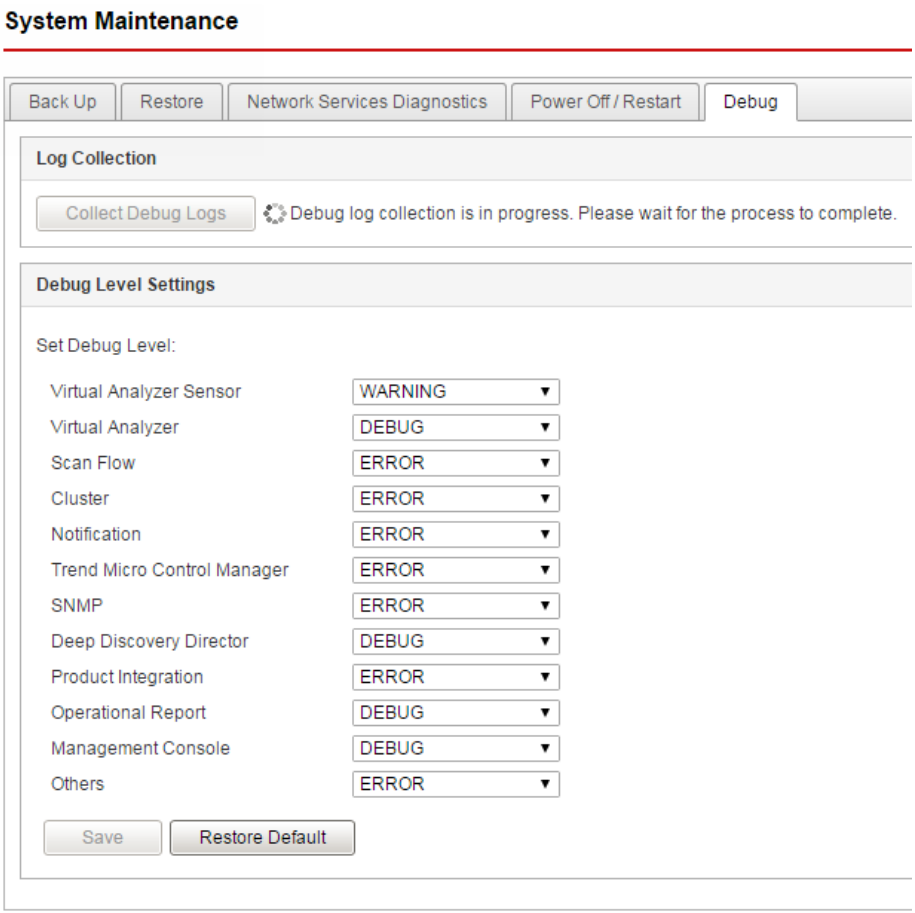
Powering off or restarting the appliance affects the following:

- Virtual Analyzer object analysis: Integrated products may queue objects or skip 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.



Debug Tab

You can use the **Debug** tab to generate and configure debug logs for troubleshooting.



Procedure

1. Specify how events will be shown in the debug logs.

a. Review the default debug levels assigned to the following events:

- Virtual Analyzer Sensor
- Virtual Analyzer
- Scan Flow
- Cluster
- Notification
- Trend Micro Control Manager
- SNMP
- Deep Discovery Director
- Product Integration
- Operational Report
- Management Console
- Others

b. To customize the debug level for the following events, click the current level assigned and select another value.

c. Click **Save**.

d. To return all debug level settings to their default values, click **Restore Default**.

2. Collect debug logs.

a. Click **Collect Debug Logs**.

b. Wait for the task to complete.

c. Click **Download Debug logs** to save the debug logs.

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
Virtual Analyzer 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. Usage instructions | Download
Manual Submission Tool	Use this tool to remotely submit samples from a local folder to Virtual Analyzer. 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.

Virtual Analyzer Image Preparation Tool

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

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

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.

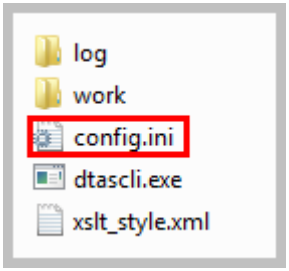
Follow the steps below to download, configure and use the Manual Submission Tool.

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`.



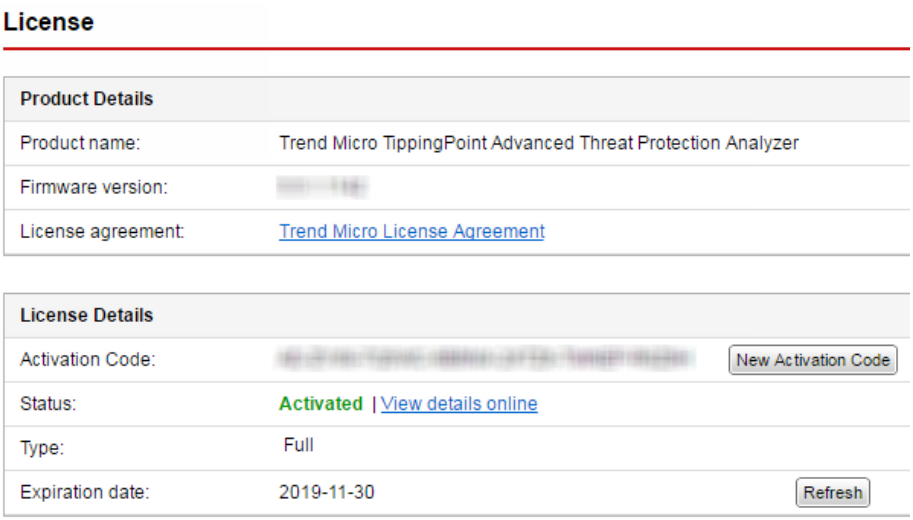
7. Next to `Host`, type the TippingPoint Advanced Threat Protection Analyzer IP address. Next to `ApiKey`, type the TippingPoint Advanced Threat Protection Analyzer API Key. Save `config.ini`.

```
[DTAS]
Host = 10.100.100.100
ApiKey = YZ12A345-B67C-890D-1E23-F45G678HIJKL
[Header]
X-DTAS-ProtocolVersion = 1.1
X-DTAS-ProductName = DTASSubmisstionTool
X-DTAS-ClientHostname = DTASSubmisstionTool01
X-DTAS-ClientUUID = e8f763c6-8db8-4d08-8bc5-8f41b
```

8. Submit the samples. For details, see *Manually Submitting Objects on page 4-15*.

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 6-18. Product Details

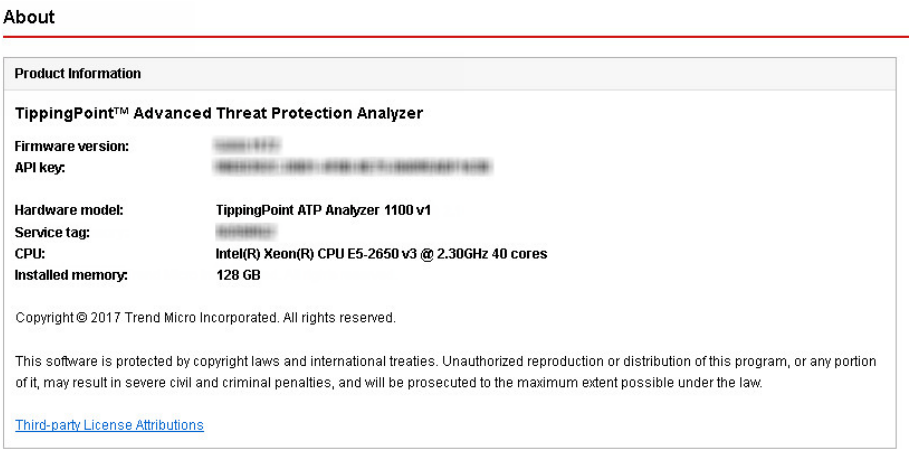
FIELD	DETAILS
Product name	Displays the name of the product.
Firmware version	Displays the full build number of the product.
License agreement	Displays a link to the **Trend Micro License Agreement**. Click the link to view or print the license agreement.

TABLE 6-19. License Details

FIELD	DETAILS
Activation Code	View the Activation Code in this section. If your license has expired, obtain a new Activation Code from Trend Micro. To renew the license, click **New Activation Code**, and type the new Activation Code. The **License** screen reappears displaying the number of days left before the product expires.
Status	Displays either **Activated**, **Not Activated**, **Grace Period**, **Expired**, or **Evaluation Expired**. Click **View details online** to view detailed license information from the Trend Micro website. If the status changes (for example, after you renewed the license) but the correct status is not indicated in the screen, click **Refresh**.
Type	• Full: Provides access to all product features • Evaluation: Provides access to all product features
Expiration date	View the expiration date of the license. Renew the license before it expires.

About Screen

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



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

   Tip

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

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

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

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia

provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

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

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

Contacting Trend Micro

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

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

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

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Web Reputation Services

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

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

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

Other Resources

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

Download Center

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

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

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

Documentation Feedback

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

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

Appendix A

Service Addresses and Ports

TippingPoint Advanced Threat Protection 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.	`atpa58-p.activeupdate.trendmicro.com/activeupdate:80` `atpa58-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.	`grid-global.trendmicro.com/ws/level-0/files: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.	`atpanalyzer580-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`
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.	`atpa580-en.fbs25.trendmicro.com:443`
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.	`atpan58-threatconnect.trendmicro.com:443`

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.	`atpa5-8-en.url.trendmicro.com:80`
		
		`atpa5-8-en-wis.trendmicro.com/wis/v1/reason:443`

Appendix B

SNMP Object Identifiers

Topics include:

- *SNMP Query Objects on page B-2*
- *SNMP Traps on page B-18*
- *Registration Objects on page B-22*

SNMP Query Objects

Table B-1. memTotalSwap

Item	Description
OID	.1.3.6.1.4.1.2021.4.3
Object name	memTotalSwap
Description	The total amount of swap space configured for this host.

Table B-2. memAvailSwap

Item	Description
OID	.1.3.6.1.4.1.2021.4.4
Object name	memAvailSwap
Description	The amount of swap space currently unused or available.

Table B-3. memTotalReal

Item	Description
OID	.1.3.6.1.4.1.2021.4.5
Object name	memTotalReal
Description	The total amount of real/physical memory installed on this host.

Table B-4. memAvailReal

Item	Description
OID	.1.3.6.1.4.1.2021.4.6
Object name	memAvailReal
Description	The amount of real/physical memory currently unused or available.

TABLE B-5. memTotalFree

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.4.11
Object name	memTotalFree
Description	The total amount of memory free or available for use on this host. This value typically covers both real memory and swap space or virtual memory.

TABLE B-6. memMinimumSwap

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.4.12
Object name	memMinimumSwap
Description	The minimum amount of swap space expected to be kept free or available during normal operation of this host. If this value (as reported by 'memAvailSwap(4)') falls below the specified level, then 'memSwapError(100)' will be set to 1 and an error message made available via 'memSwapErrorMsg(101)'.

TABLE B-7. memShared

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.4.13
Object name	memShared
Description	The total amount of real or virtual memory currently allocated for use as shared memory. This object will not be implemented on hosts where the underlying operating system does not explicitly identify memory as specifically reserved for this purpose.

TABLE B-8. memBuffer

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.4.14

Item	Description
Object name	memBuffer
Description	The total amount of real or virtual memory currently allocated for use as memory buffers. This object will not be implemented on hosts where the underlying operating system does not explicitly identify memory as specifically reserved for this purpose.

Table B-9. memCached

Item	Description
OID	.1.3.6.1.4.1.2021.4.15
Object name	memCached
Description	The total amount of real or virtual memory currently allocated for use as cached memory. This object will not be implemented on hosts where the underlying operating system does not explicitly identify memory as reserved for this purpose.

Table B-10. memSwapError

Item	Description
OID	.1.3.6.1.4.1.2021.4.100
Object name	memSwapError
Description	Indicates whether the amount of available swap space (as reported by 'memAvailSwap(4)') is less than the minimum (specified by 'memMinimumSwap(12)').

Table B-11. memSwapErrorMsg

Item	Description
OID	.1.3.6.1.4.1.2021.4.101
Object name	memSwapErrorMsg
Description	Describes whether the amount of available swap space (as reported by 'memAvailSwap(4)') is less than the minimum (specified by 'memMinimumSwap(12)').

TABLE B-12. dskIndex

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.1
Object name	dskIndex
Description	Integer reference number (row number) for the disk mib.

TABLE B-13. dskPath

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.2
Object name	dskPath
Description	Path where the disk is mounted.

TABLE B-14. dskDevice

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.3
Object name	dskDevice
Description	Path of the device for the partition.

TABLE B-15. dskMinimum

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.4
Object name	dskMinimum
Description	Minimum space required on the disk (in kBytes) before the errors are triggered. Either this or dskMinPercent is configured via the agent's snmpd.conf file.

TABLE B-16. dskMinPercent

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.5
Object name	dskMinPercent
Description	Percentage of minimum space required on the disk before the errors are triggered. Either this or dskMinimum is configured via the agent's snmpd.conf file.

TABLE B-17. dskTotal

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.6
Object name	dskTotal
Description	Total size of the disk/partion (kBytes).

TABLE B-18. dskAvail

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.7
Object name	dskAvail
Description	Available disk space.

TABLE B-19. dskUsed

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.8
Object name	dskUsed
Description	Disk space used.

TABLE B-20. dskPercent

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.9
Object name	dskPercent
Description	Percentage of space used on disk.

TABLE B-21. dskPercentNode

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.10
Object name	dskPercentNode
Description	Percentage of inodes used on disk.

TABLE B-22. dskErrorFlag

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.100
Object name	dskErrorFlag
Description	Error flag indicating that the disk or partition is under the minimum required space configured for it.

TABLE B-23. dskErrorMsg

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.9.1.101
Object name	dskErrorMsg
Description	A text description providing a warning and the space left on the disk.

TABLE B-24. ssSwapIn

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.3
Object name	ssSwapIn
Description	The average amount of memory swapped in from disk, calculated over the last minute.

TABLE B-25. ssSwapOut

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.4
Object name	ssSwapOut
Description	The average amount of memory swapped out to disk, calculated over the last minute.

TABLE B-26. ssIOSent

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.5
Object name	ssIOSent
Description	The average amount of data written to disk or other block devices, calculated over the last minute. This object has been deprecated in favour of 'ssIORawSent(57)', which can be used to calculate the same metric, but over any desired time period.

TABLE B-27. ssIOReceive

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.6
Object name	ssIOReceive

Item	Description
Description	The average amount of data read from disk or other block devices, calculated over the last minute. This object has been deprecated in favour of 'ssIORawReceived(58)', which can be used to calculate the same metric, but over any desired time period.

Table B-28. ssSysInterrupts

Item	Description
OID	.1.3.6.1.4.1.2021.11.7
Object name	ssSysInterrupts
Description	The average rate of interrupts processed (including the clock) calculated over the last minute. This object has been deprecated in favour of 'ssRawInterrupts(59)', which can be used to calculate the same metric, but over any desired time period.

Table B-29. ssSysContext

Item	Description
OID	.1.3.6.1.4.1.2021.11.8
Object name	ssSysContext
Description	The average rate of context switches, calculated over the last minute. This object has been deprecated in favour of 'ssRawContext(60)', which can be used to calculate the same metric, but over any desired time period.

Table B-30. ssCpuUser

Item	Description
OID	.1.3.6.1.4.1.2021.11.9
Object name	ssCpuUser

Item	Description
Description	The percentage of CPU time spent processing user-level code, calculated over the last minute. This object has been deprecated in favour of 'ssCpuRawUser(50)', which can be used to calculate the same metric, but over any desired time period.

Table B-31. ssCpuSystem

Item	Description
OID	.1.3.6.1.4.1.2021.11.10
Object name	ssCpuSystem
Description	The percentage of CPU time spent processing system-level code, calculated over the last minute. This object has been deprecated in favour of 'ssCpuRawSystem(52)', which can be used to calculate the same metric, but over any desired time period.

Table B-32. ssCpuIdle

Item	Description
OID	.1.3.6.1.4.1.2021.11.11
Object name	ssCpuIdle
Description	The percentage of processor time spent idle, calculated over the last minute. This object has been deprecated in favour of 'ssCpuRawIdle(53)', which can be used to calculate the same metric, but over any desired time period.

Table B-33. ssCpuRawUser

Item	Description
OID	.1.3.6.1.4.1.2021.11.50
Object name	ssCpuRawUser
Description	The number of 'ticks' (typically 1/100s) spent processing user-level code. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-34. ssCpuRawNice

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.51
Object name	ssCpuRawNice
Description	The number of 'ticks' (typically 1/100s) spent processing reduced-priority code. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-35. ssCpuRawSystem

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.52
Object name	ssCpuRawSystem
Description	The number of 'ticks' (typically 1/100s) spent processing system-level code. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors). This object may sometimes be implemented as the combination of the 'ssCpuRawWait(54)' and 'ssCpuRawKernel(55)' counters, so care must be taken when summing the overall raw counters.

TABLE B-36. ssCpuRawIdle

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.53
Object name	ssCpuRawIdle
Description	The number of 'ticks' (typically 1/100s) spent idle. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-37. ssCpuRawWait

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.54
Object name	ssCpuRawWait
Description	The number of 'ticks' (typically 1/100s) spent waiting for IO. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. This time may also be included within the 'ssCpuRawSystem(52)' counter. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-38. ssCpuRawKernel

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.55
Object name	ssCpuRawKernel
Description	The number of 'ticks' (typically 1/100s) spent processing kernel-level code. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. This time may also be included within the 'ssCpuRawSystem(52)' counter. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

TABLE B-39. ssCpuRawInterrupt

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.2021.11.56
Object name	ssCpuRawInterrupt

Item	Description
Description	The number of 'ticks' (typically 1/100s) spent processing hardware interrupts. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

Table B-40. ssIORawSent

Item	Description
OID	.1.3.6.1.4.1.2021.11.57
Object name	ssIORawSent
Description	Number of blocks sent to a block device.

Table B-41. ssIORawReceived

Item	Description
OID	.1.3.6.1.4.1.2021.11.58
Object name	ssIORawReceived
Description	Number of blocks received from a block device.

Table B-42. ssRawInterrupts

Item	Description
OID	.1.3.6.1.4.1.2021.11.59
Object name	ssRawInterrupts
Description	Number of interrupts processed.

Table B-43. ssRawContexts

Item	Description
OID	.1.3.6.1.4.1.2021.11.60

Item	Description
Object name	ssRawContexts
Description	Number of context switches.

Table B-44. ssCpuRawSoftIRQ

Item	Description
OID	.1.3.6.1.4.1.2021.11.61
Object name	ssCpuRawSoftIRQ
Description	The number of 'ticks' (typically 1/100s) spent processing software interrupts. This object will not be implemented on hosts where the underlying operating system does not measure this particular CPU metric. On a multi-processor system, the 'ssCpuRaw*' counters are cumulative over all CPUs, so their sum will typically be N*100 (for N processors).

Table B-45. ssRawSwapIn

Item	Description
OID	.1.3.6.1.4.1.2021.11.62
Object name	ssRawSwapIn
Description	Number of blocks swapped in.

Table B-46. ssRawSwapOut

Item	Description
OID	.1.3.6.1.4.1.2021.11.63
Object name	ssRawSwapOut
Description	Number of blocks swapped out.

TABLE B-47. productVersion

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.1.1
Object name	productVersion
Description	Returns the TippingPoint Advanced Threat Protection Analyzer version.

TABLE B-48. productBuild

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.1.2
Object name	productBuild
Description	Returns the TippingPoint Advanced Threat Protection Analyzer build number.

TABLE B-49. productHotfix

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.1.3
Object name	productHotfix
Description	Returns the TippingPoint Advanced Threat Protection Analyzer hotfix number.

TABLE B-50. componentTable

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.2
Object name	componentTable
Description	A table containing a set of component information.

TABLE B-51. componentIndex

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.2.1.1
Object name	componentIndex
Description	Returns the component index.

TABLE B-52. componentID

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.2.1.2
Object name	componentID
Description	Returns the component ID.

TABLE B-53. componentName

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.2.1.3
Object name	componentName
Description	Returns the component name.

TABLE B-54. componentVersion

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.2.1.4
Object name	componentVersion
Description	Returns the component version.

TABLE B-55. throughputTable

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.1.3

Item	Description
Object name	throughputTable
Description	A table containing a set of throughput information.

Table B-56. ifIndex

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.3.1.1
Object name	ifIndex
Description	Returns the interface index.

Table B-57. ifDescr

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.3.1.2
Object name	ifDescr
Description	Returns the interface description.

Table B-58. ifReceiveThroughput

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.3.1.3
Object name	ifReceiveThroughput
Description	Returns the interface receiving throughput.

Table B-59. ifTransmitThroughput

Item	Description
OID	.1.3.6.1.4.1.6101.3005.1.3.1.4
Object name	ifTransmitThroughput
Description	Returns the interface transmitting throughput.

SNMP Traps

Table B-60. coldStart

Item	Description
OID	.1.3.6.1.6.3.1.1.5.1.0
Object name	coldStart
Description	A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.

Table B-61. linkDown

Item	Description
OID	.1.3.6.1.6.3.1.1.5.3.0
Object name	linkDown
Description	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.

Table B-62. linkUp

Item	Description
OID	.1.3.6.1.6.3.1.1.5.4.0
Object name	linkUp
Description	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.

TABLE B-63. nsNotifyShutdown

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.8072.4.0.2
Object name	nsNotifyShutdown
Description	An indication that the agent is in the process of being shut down.

TABLE B-64. accountLockedNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.1
Object name	accountLockedNotification
Description	A notification for when an account was locked because of multiple unsuccessful logon attempts.

TABLE B-65. vaStoppedNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.2
Object name	vaStoppedNotification
Description	A notification for when Virtual Analyzer is unable to recover from an error.

TABLE B-66. vaLongQueueNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.3
Object name	vaLongQueueNotification
Description	A notification for when the number of Virtual Analyzer submissions has exceeded the threshold.

TABLE B-67. compUpdateErrorNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.4
Object name	compUpdateErrorNotification
Description	A notification for when a component update was unsuccessful.

TABLE B-68. highCpuNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.5
Object name	highCpuNotification
Description	A notification for when the average CPU usage in the last 5 minutes has exceeded the threshold.

TABLE B-69. highMemNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.6
Object name	highMemNotification
Description	A notification for when the average memory usage in the last 5 minutes has exceeded the threshold.

TABLE B-70. highDiskNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.7
Object name	highDiskNotification
Description	A notification for when disk usage has exceeded the threshold.

TABLE B-71. secondaryDownNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.8
Object name	secondaryDownNotification
Description	A notification for when a secondary appliance is unable to recover from an error.

TABLE B-72. haPassiveActivatedNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.9
Object name	haPassiveActivatedNotification
Description	A notification for when the active primary appliance is unable to recover from an error, and the passive primary appliance has taken over the active role.

TABLE B-73. haSuspendedNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.10
Object name	haSuspendedNotification
Description	A notification for when the passive primary appliance is unable to recover from an error, and high availability is suspended.

TABLE B-74. syslogErrorNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.11
Object name	syslogErrorNotification
Description	A notification for when the syslog server is inaccessible.

TABLE B-75. backupErrorNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.12
Object name	backupErrorNotification
Description	A notification for when the backup server is inaccessible.

TABLE B-76. haRestoredNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.13
Object name	haRestoredNotification
Description	A notification for when the passive primary appliance has recovered and high availability has been restored.

TABLE B-77. vaHighRiskNotification

ITEM	DESCRIPTION
OID	.1.3.6.1.4.1.6101.3005.2.1.0.14
Object name	vaHighRiskNotification
Description	A notification for when the number of new high-risk objects identified during the last TimeRange has reached the threshold.

Registration Objects

OID	DESCRIPTION
.1.3.6.1.4.1.2021	UC Davis
.1.3.6.1.4.1.6101	Trend Micro, Inc.
.1.3.6.1.6.3.1.1.5.1	SNMPv2-MIB MIB
.1.3.6.1.4.1.8072	NET-SNMP-AGENT-MIB

Index

A

account management, 6-57
Activation Code, 6-74
administration, 4-44
    archive file passwords, 4-44
Advanced Threat Scan Engine, 5-21, 6-2
alerts, 5-3–5-5, 5-7–5-17
    critical alerts, 5-3
    important alerts, 5-4
    informational alerts, 5-5
    notification parameters, 5-7–5-17
API key, 6-77
ATSE, 5-21, 6-2
average Virtual Analyzer queue time alert, 5-4

C

C&C list, 4-23
components, 6-2
contact management, 6-61
CPU usage alert, 5-4
critical alerts, 5-3, 5-7
customized alerts and reports, 5-32

D

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

E

email scanning
    archive file passwords, 4-44
exceptions, 4-29

G

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

I

images, 4-35, 4-36
important alerts, 5-4, 5-8–5-16
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, 6-74
license expiration alert, 5-3
log settings, 6-13
    syslog server, 6-13

M

management console, 2-2
    navigation, 2-4
    session duration, 6-41
management console accounts, 6-57
message delivery alert, 5-4

N

Network Content Correlation Pattern, 6-3
Network Content Inspection Engine, 6-3
Network Content Inspection 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, 4-35, 4-36
sandbox instances, 4-37
sandbox management, 4-33
    archive passwords, 4-43
    images, 4-35
        importing, 4-36
        modifying instances, 4-37
    image status, 4-34
    network connection, 4-50
    Virtual Analyzer status, 4-34
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
support
    resolve issues faster, 7-4
suspicious objects, 4-23
syslog server, 6-13
system maintenance, 6-63
    back up tab, 6-64
        configuration settings backup, 6-64
        data backup, 6-66
    cluster tab
        primary appliance, 6-53
        remove, 6-53
        secondary appliance, 6-51, 6-53
        test connection, 6-51
    nodes list, 6-44
    restore tab, 6-67
system settings, 6-26
    Network Tab, 6-27
    Password Policy Tab, 6-40
    power off / restart tab, 6-69
    Proxy Tab, 6-28
    Session Timeout Tab, 6-41
    Time Tab, 6-31

T

tabs, 3-3
third-party licenses, 6-77
tools, 6-72

U

unreachable relay MTA alert, 5-3
update completed surge, 5-5
update failed alert, 5-4
updates, 6-2
    components, 6-2
    firmware, 6-11
    update settings, 6-5

V

Virtual Analyzer, 4-2, 4-44
    archive file passwords, 4-44

Virtual Analyzer Configuration Pattern, 6-4
Virtual Analyzer Sensors, 6-4

W

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

Y

YARA rule file
    create, 4-40
    requirements, 4-40

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: APEM57793/170411